kuppingercole
ANALYSTS

Web Application and API Protection

Osman Celik

August 25, 2025

LEADERSHIP
COMPASS
2025

This report provides an overview of the WAAP market and a compass to help you find a solution that best meets your needs. It examines solutions that provide an integrated set of security and compliance capabilities designed to protect cloud-native applications across the development and production lifecycle. It provides an assessment of the capabilities of these solutions to meet the needs of all organizations to monitor, assess, and manage these risks.

Contents

Executive Summary

Web applications are the backbone of many digital services. They support activities like online banking, e-commerce, and internal business systems. APIs allow two software components to interact and exchange data by following predefined definitions and communication protocols. As organizations depend more on interconnected, API-driven architectures, protecting these important interfaces has become much more complex than what traditional web traffic inspection can manage. What was once primarily the job of Web Application Firewalls (WAFs) has now expanded into a wider category, called Web Application and API Protection (WAAP).

The WAAP market reflects a convergence of security controls that defend modern applications not only against common threats but also against sophisticated bot-driven abuse, API misuse, business logic exploitation, and Layer 7 (L7) Distributed Denial of Service (DDoS) attacks. WAAP platforms now integrate core WAF functions with API discovery and protection, bot management, and DDoS protection, often enhanced by cyber threat intelligence (CTI), machine learning (ML), artificial intelligence (AI), and real-time behavioral analysis. This change is not just a simple upgrade from WAFs, but a new approach to delivering, scaling, and integrating application-layer security in cloud-native, hybrid, and container settings.

Modern WAAP solutions need to support API protocols, apply schema validation, identify undocumented endpoints, and enforce rate limiting. They should also support microservices and CI/CD pipelines. In parallel, effective bot management is no longer limited to signature-based detection but requires behavioral biometrics to distinguish between benign bots, malicious automation, and legitimate traffic. The most comprehensive solutions offer support for Content Delivery Networks (CDNs), data masking, vulnerability scanning, virtual patching, fraud prevention, and threat telemetry correlation. They should be also designed to lower operational costs through automation and unified policy management.

As more applications operate across different cloud environments, from public cloud to edge networks, WAAP vendors are expected to provide flexible and scalable delivery models that support SaaS, IaaS agents, containers, and multi-cloud deployments. Performance, ease of integration, and compatibility with DevSecOps practices are now essential. While many WAAP vendors come from traditional WAF backgrounds, the current landscape features a variety of players, including global cloud providers, CDN-based edge vendors, cybersecurity-focused vendors, and startups with specialized skills in web application and API defense. However, the market is not very dynamic.

The expected shift from WAF to more complete WAAP solutions has occurred in the market. Vendors are now focusing on merging traditional WAF features with tools that support API discovery and protection. These capabilities not only increase coverage but also allow security teams to apply granular policies at the API level, which aligns with modern application architectures. As APIs continue to play a significant role in digital service interfaces, the relevance of WAAP will expand beyond threat detection to include visibility and control.

Organizations are adopting WAAP solutions to protect against sophisticated threats that target both traditional and modern infrastructures. The market drivers include growing API exposure, bot abuse, and stricter compliance requirements. The WAAP market has gained global relevance as large enterprises and small and medium-sized businesses (SMBs) seek integrated solutions that extend beyond legacy WAFs. While larger organizations often require flexible deployment options and advanced data analytics, modular offerings have also become available for mid-sized businesses. WAAP market is especially relevant for industries that handle sensitive data or high volumes of transactions, such as finance, retail, healthcare, insurance, government, and e-commerce where secure application access is essential to both operational continuity and customer trust.

This KuppingerCole Leadership Compass covers solutions that protect web applications and APIs through Web Application and API Protection (WAAP) platforms. These offerings are deployed across organizations of varying sizes and are expected to meet foundational WAF capabilities while extending coverage to modern threats targeting APIs, and complex application environments. In addition to core capabilities, the evaluated solutions address emerging threats and innovative capabilities. For more information about the methodology guiding this analysis, please refer to KuppingerCole’s Research Methodology.

Key Findings

- Unlike traditional WAF, WAAP takes a broader security approach, addressing not only threats to web traffic, but also advanced risks related to APIs.
- The main capabilities of WAAP include WAF, API discovery and protection, bot management, and DDoS protection.
- Effective bot management within WAAP requires ML-driven detection models that differentiate between benign bots, malicious bots, and legitimate traffic.
- In this paper, we use the term "API discovery and protection" since WAAP provides runtime defenses, such as validation and anomaly detection, but lacks full lifecycle features. WAAP mainly serves as an enforcement layer, and dedicated API security tools remain necessary for complete coverage.
- WAAP platforms include out-of-the-box controls for credential stuffing, scraping, account takeover (ATO), brute-force login attempts, and session hijacking.
- Solutions utilize a combination of static signatures, heuristic analysis, contextual behavior detection, and supervised/unsupervised ML for threat mitigation.
- CAPTCHA, passive biometrics, fingerprinting, JavaScript, and silent (invisible) challenges are used to validate traffic authenticity and mitigate bots.
- Web acceleration and CDN support appear as a differentiator among vendors.
- Some WAAP vendors have begun integrating agentic AI into their platforms to enhance decision-making in areas such as adaptive threat response and anomaly detection.
- WAAP solutions are offered through various delivery models: SaaS, on-premises, hybrid, edge-based, container-native, and fully managed services.
- The WAAP market is considered mature, with core functionalities standardized across leading vendors.

- WAAP is adopted by organizations of all sizes, from SMBs to large enterprises, across global regions.
- Industries such as finance, healthcare, e-commerce, insurance, and government are particularly dependent on WAAP to ensure secure and compliant application delivery.
- The WAAP market features global cloud providers (e.g., AWS, Google), CDN/edge vendors (e.g., Fastly, Akamai), traditional security vendors (e.g., Fortinet, Check Point), and focused startups (e.g., Prophaze, Sense Defense).
- The vendor landscape includes legacy WAF providers expanding into WAAP, cloud-native entrants, and startups focusing on specific WAAP functions.
- Entry barriers for startups are high due to the complexity and breadth of WAAP functionality.
- The Overall Leaders (in alphabetical order) are AWS, F5, Fastly, Google, Imperva, and Radware.

Market Analysis

WAAP solutions extend the scope of traditional WAFs by incorporating more functions, particularly around API security, ML-driven bot management, and L7 DDoS mitigation. While WAFs primarily rely on rule-based inspection of HTTP requests to detect and block known attack vectors, WAAP platforms are typically designed to address emerging attack vectors. WAAP's API security features make it more effective for protecting modern IT environments where both web applications and APIs are exposed to more internal and external threats.

WAAP solutions provide runtime protections for APIs, but they do not cover the full API lifecycle or offer the same depth as specialized API security platforms. That is why rather than API security, we often use the term "API discovery and protection" in this paper. WAAP capabilities generally include request validation, anomaly detection, and abuse prevention mechanisms. However, they lack features such as automated inventory across internal and external APIs, full version control, deep business logic analysis. As a result, WAAP can act as an enforcement layer in API security architectures. However, in environments with extensive API exposure, organizations still need dedicated and advanced API security tools for complete coverage.

Most WAAP platforms incorporate mechanisms to detect and mitigate automated traffic and application-layer DDoS events. This reflects how often automated threats occur, such as credential stuffing, scraping, and synthetic account generation. These threats target both web applications and exposed APIs. WAAP vendors typically use heuristic, signature-based, and behavioral analysis approaches, sometimes supported by supervised or unsupervised ML models. These mechanisms are used to apply policy controls such as request blocking, rate limiting, or user verification through CAPTCHA or passive fingerprinting. Ultimately, adding these capabilities to the WAAP architecture decreases the need for separate tools to manage automated threats.

In recent years, several established WAAP vendors have expanded their product capabilities through acquisitions. F5 acquired both Wib and LeakSignal to strengthen its API security and runtime data governance features, and Lilac Cloud for CDN delivery. In 2024, Akamai completed the acquisition of API security company Noname Security for about $450 million. This acquisition is aimed at strengthening Akamai's WAAP stack with capabilities for discovering shadow APIs and evidence-based vulnerability detection and testing. In late 2023, Thales finalized its acquisition of Imperva, a major player in the WAAP market. Also in 2024, Link11 acquired Reblaze, a WAAP vendor previously featured in last year's Leadership Compass report. These examples show a clear trend in WAAP market, as established vendors are acquiring specialized companies to close technical gaps.

While the WAAP market has become more standardized, some early-stage vendors such as Prophaze continue to enter the market. Startups that focus on lightweight deployment models and API discovery can still gain traction. However, entry barriers to this market remain high due the complexity of core WAAP capabilities. Most startups fail to offer a complete suite of WAAP. That is why they are trying to differentiate based on narrow functional areas rather than compete across the full WAAP stack. At KuppingerCole Analysts, we believe that the WAAP market is mature. The functional overlap between vendors has reduced differentiation, and baseline requirements now necessitate unique and innovative capabilities (see our required capabilities list below). New entrants must compete on technology, deployment flexibility, operational costs, and integration capability. This makes entering the market more resource-intensive and limits it to vendors with narrow specialties or new technical solutions.

Market Segmentation

This KuppingerCole Leadership Compass covers solutions that protect web applications, APIs, and their associated data using WAAP technologies, which are adopted by organizations of all sizes. These solutions must not only meet the foundational WAF requirements seen in the past but also offer advanced capabilities that address modern security challenges, particularly in API security, bot mitigation, and CTI.

Traditional WAF solutions focused primarily on protecting web applications through rule-based filtering, DDoS protection, signature-based attack detection, and traffic monitoring. However, the rapid growth of APIs, cloud-native architectures, and microservices has introduced new attack vectors that require a more sophisticated approach. Consequently, WAAP solutions must extend beyond traditional WAF capabilities.

The WAAP market has moved beyond static rule-based defenses, adopting dynamic, intelligent mechanisms such as behavioral anomaly detection, ML-driven bot mitigation, API security posture management, automated policy enforcement, and CI/CD integration for DevSecOps. WAAP solutions also enhance security with runtime API protection, fraud detection, access control, compliance enforcement (e.g., EU GDPR, NIS2, and PCI DSS), and performance optimization through adaptive rate limiting. Over the past three years, we have shown that modern WAF requirements have already evolved to include advanced capabilities. These include ML-driven threat intelligence, monitoring, detection, device fingerprinting, bot and mobile app protection, vulnerability remediation, Data Loss Prevention (DLP), virtual patching, zero-day protection, and performance enhancements such as CDN and content acceleration.

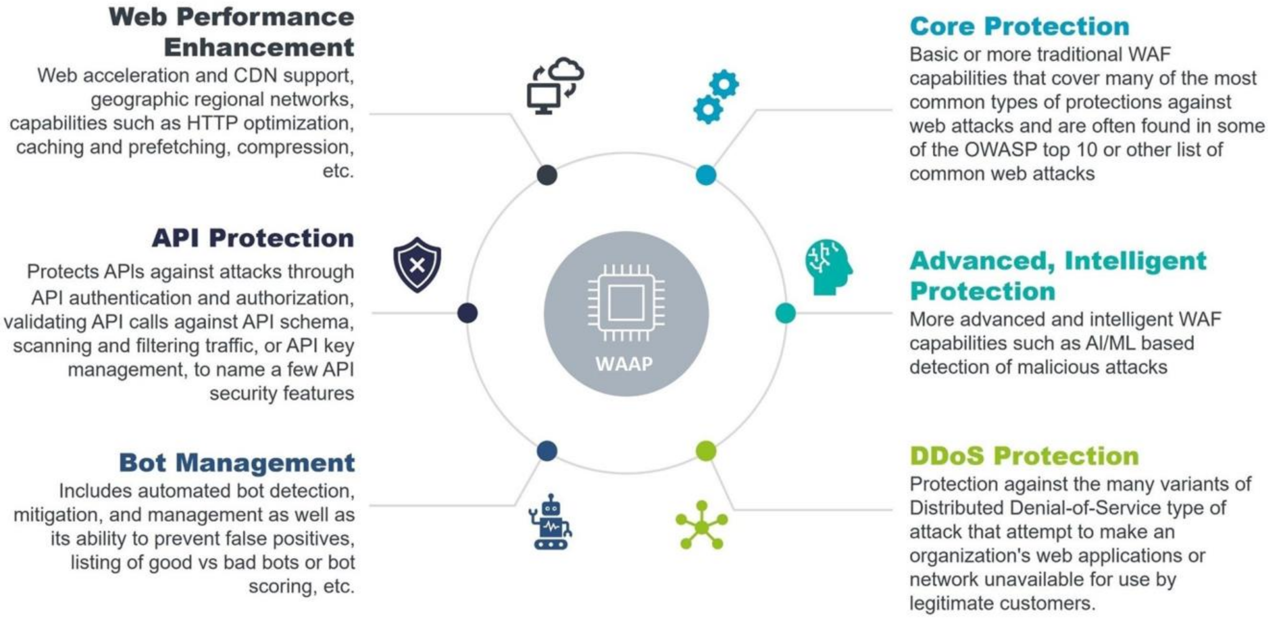
This Leadership Compass specifically evaluates the WAAP market as a distinct segment by recognizing its evolution from traditional WAF technologies. While the foundational security principles remain, WAAP solutions differentiate themselves through their ability to extend their protection to APIs, identify sophisticated bot activity, leverage threat intelligence, and support flexible deployment models across on-premises, cloud, and hybrid environments.

Furthermore, some solutions offer managed security services to enhance threat monitoring, automated remediation, and incident response. As organizations continue to adopt modern, loosely coupled and highly distributed application architectures, securing them requires a proactive and adaptive security framework. This report evaluates WAAP vendors based on their ability to meet these modern requirements.

Thus, this Leadership Compass analyzes the WAAP solutions' ability to provide:

- Coverage for OWASP Top 10 vulnerabilities for both web applications and APIs. This includes protection against emerging and common attack vectors.
- Protection against complex and evolving attack patterns, including automated threats, malicious bots, API abuse, and business logic attacks. The solution should differentiate between good and bad bot traffic using AI/ML-driven behavioral analysis.
- Leveraging real-time threat intelligence to detect and respond to emerging threats. The solution should integrate with external threat feeds.
- Securing popular API protocols such as REST, SOAP, GraphQL, and gRPC, and include API discovery and protection capabilities, such as those defined by OWASP API Security Top 10.
- Advanced fraud detection capabilities to mitigate ATO, credential stuffing, brute force login attempts, and session hijacking.
- AI-driven analytics help detect anomalies in access patterns and automate risk scoring.
- A unified, single-pane-of-glass dashboard providing real-time visibility into attack trends, API traffic analysis, monitoring of web applications, risk scoring, and alert prioritization. Customizable dashboards should allow teams to track key security metrics, compliance status, and response actions.
- Support for various deployment models, including on-premises, cloud, multi-cloud, hybrid environments, containerized architectures, as well as integration with existing CI/CD pipelines and DevSecOps workflows.
- A modern, scalable architecture leveraging microservices, cloud-native principles, and adaptive scaling to handle high traffic loads. WAAP solutions should support edge-based protection, CDN integration, and caching mechanisms.
- A full set of APIs exposing all WAAP functionalities for automation, integration, and orchestration within security workflows.
- Detailed audit logging, forensics, and compliance reporting capabilities aligned with major cybersecurity frameworks such as PCI-DSS, NIS2, and SOC 2, and privacy regulations such as GDPR and CCPA. Solutions should offer pre-built and customizable compliance reports.

- Additional capabilities such as Attribute-Based Access Control (ABAC), Policy-Based Access Control (PBAC), policy customization, security automation, and integration with SIEM/SOAR solutions.



Web Performance Enhancement
Web acceleration and CDN support, geographic regional networks, capabilities such as HTTP optimization, caching and prefetching, compression, etc.

API Protection
Protects APIs against attacks through API authentication and authorization, validating API calls against API schema, scanning and filtering traffic, or API key management, to name a few API security features

Bot Management
Includes automated bot detection, mitigation, and management as well as its ability to prevent false positives, listing of good vs bad bots or bot scoring, etc.

Core Protection
Basic or more traditional WAF capabilities that cover many of the most common types of protections against web attacks and are often found in some of the OWASP top 10 or other list of common web attacks

Advanced, Intelligent Protection
More advanced and intelligent WAF capabilities such as AI/ML based detection of malicious attacks

DDoS Protection
Protection against the many variants of Distributed Denial-of-Service type of attack that attempt to make an organization's web applications or network unavailable for use by legitimate customers.

Figure 1: WAAP Capabilities

Delivery Models

The WAAP market continues to move away from traditional on-premises setups toward cloud-native, service-oriented models. This trend is driven by the increasing need for complete API protection, better bot management, and easy integration with modern CI/CD pipelines. However, some customers still prefer on-premises products for specific reasons within their organizations. These reasons include data sovereignty, ultra-low latency, regulatory constraints, or air-gapped network environments. Because of this, we can assume that a hybrid or multi-cloud delivery model will be the best option for the future.

Cloud-based WAAP (SaaS) platforms suit organizations that value agility and flexibility. They often provide elastic scalability, centralized policy management, and quick deployment. These solutions typically come as globally distributed services through vendor-managed Points of Presence (PoPs) or CDNs.

On-premises WAAP solutions provide maximum control. They work well for organizations with strict compliance requirements, such as healthcare and finance, as well as for those needing data residency or custom traffic inspection logic. Organizations with legacy systems or sensitive workloads that cannot connect to external networks often prefer these deployments.

Hybrid WAAP architectures blend cloud-based platforms with on-premises enforcement points. This setup allows organizations to use cloud automation while keeping important inspection and enforcement close to the application infrastructure. This model works well for gradual cloud migration strategies or for organizations with varied IT environments.

Edge-delivered WAAP is a delivery model where protection occurs at edge nodes closest to the user, often using CDN or distributed edge networks. This approach cuts down latency, boosts performance, and suits globally distributed applications and microservices.

Containerized and Kubernetes-native WAAP offerings are also becoming popular as organizations deploy more applications in cloud-native environments. In such environments, security tools must integrate with microservices, scale dynamically, and provide protection across distributed workloads.

Managed WAAP services provide organizations with a fully or partially outsourced model. In this setup, a third-party provider or the WAAP vendor takes care of deploying, configuring, tuning, and operating WAAP solutions. This model is particularly helpful for organizations that do not have in-house security knowledge or operational resources.

Each deployment option has its own advantages and drawbacks. The right choice depends on the specific needs of the organization, application architecture, API exposure level, DevSecOps maturity, real-time protection needs, compliance requirements, and IT infrastructure strategy.

Required Capabilities

The core capabilities of WAAP are:

- Denial of Service (DoS) and DDoS Protection.
- Signature- and rule-based detection of malicious web and API traffic.
- OWASP Top 10 protections for both web applications and APIs.
- Logging of HTTP and API transactions, events, and notifications of all suspicious traffic for forensic tracking and incident response.
- Reporting (e.g., audit, forensics, compliance, API-specific security monitoring, etc.).
- Centralized management (a single-pane dashboard providing visibility into threats, API traffic, policy enforcement, attack trends, and response actions).
- Advanced bot management (AI-driven bot detection and mitigation, distinguishing between benign and bad bot traffic).
- Comprehensive API inventory and runtime protection (automatic API discovery, schema validation, authentication enforcement, and protection against API abuse).
- Cyber threat intelligence (real-time intelligence feeds, IP reputation scoring, AI-driven anomaly detection, and predictive attack analytics).
- Security orchestration/integration with Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) solutions.
- Adaptive rate limiting (automated rate control to prevent API abuse and volumetric attacks).
- Zero-Day attack protection
- DevSecOps integration

- CDN or web/content acceleration

Innovative capabilities that we would like to see a WAAP vendor offering are:

- Support for hybrid IT environments
- WAAP delivery models (support for cloud-native, on-premises, managed services, and API security gateways)
- Integration with third-party security solutions such as threat intelligence platforms, analytics, web fraud detection services, and Extended Detection and Response (XDR)
- WAAP policy management (granular policy enforcement, real-time updates, and automated rule adaptation)
- Compliance enforcement
- Support for containers, Kubernetes, and other microservice environments
- DLP
- Virtual patching
- Mobile app protection
- Fraud detection and account takeover protection (AI-driven risk scoring, credential stuffing prevention, and behavioral analytics)
- API attack surface management
- AI-powered automated API threat hunting

Leadership

Selecting a vendor of a product or service must not only be based on the information provided in a KuppingerCole Leadership Compass. The Leadership Compass provides a comparison based on standardized criteria and can help identify vendors that shall be further evaluated. However, a thorough selection includes a subsequent detailed analysis and a Proof of Concept of pilot phase, based on the specific criteria of the customer.

Based on our rating, we created various Leadership ratings. The Overall Leadership rating provides a combined view of the ratings for

- Product Leadership
- Innovation Leadership
- Market Leadership

Overall Leadership

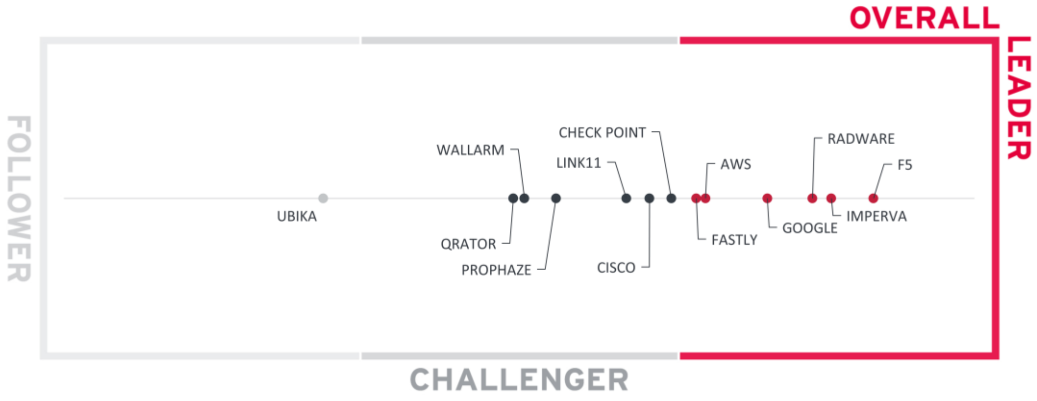


Figure 2: Overall Leadership in the WAAP market

The Overall Leadership chart is linear, with Followers appearing on the left side, Challengers in the center, and Leaders on the right. The rating provides a consolidated view of all-around functionality, market presence, and financial security.

However, these vendors may differ significantly from each other in terms of product features, innovation, and market leadership. Therefore, we recommend considering our other leadership categories in the sections covering each vendor and their products to get a comprehensive understanding of the players in this market and which of your use cases they support best.

In the Overall Leadership category, F5, Imperva, and Radware are the top-ranked vendors, with Google, AWS, and Fastly following them.

In the Overall Challengers section, Check Point, Cisco, and Link11 are positioned close to crossing into Overall Leadership. Rounding out the list of challengers are Prophaze, Wallarm, and Qrator Labs.

UBIKA is the only follower in this Overall Leadership rating.

Overall Leaders are (in alphabetical order):

- AWS
- F5
- Fastly
- Google
- Imperva
- Radware

Product Leadership

Product leadership is the first specific category examined below. This view is mainly based on the presence and completeness of required features as defined in the required capabilities section above. The vertical axis shows the product strength plotted against the combined/overall strength on the horizontal axis. The Product Leadership chart is rectangular and divided into thirds. Product Leaders occupy the top section. Challengers are in the center. Followers are in the lower section.

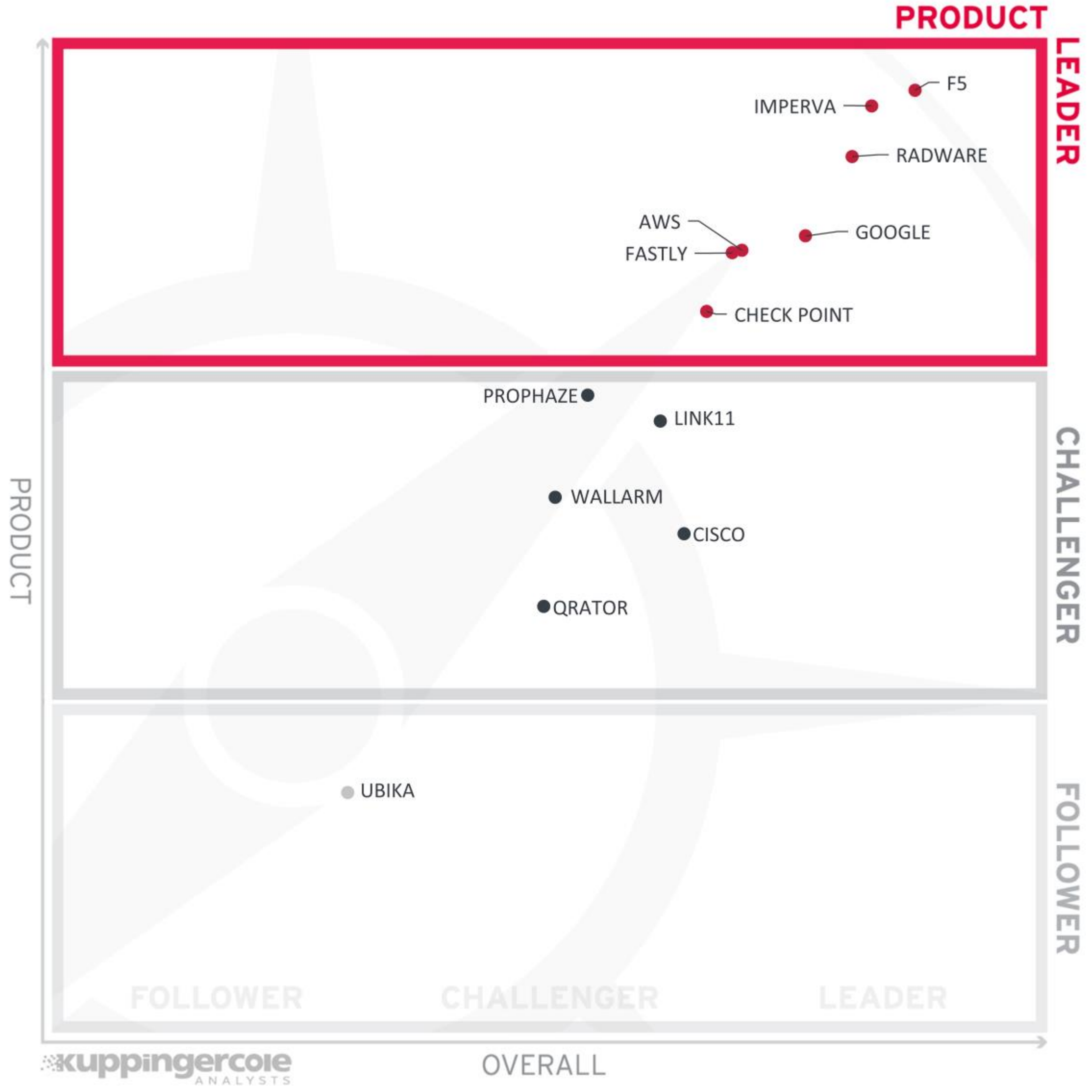


Figure 3: Product Leadership in the WAAP market

In the Product Leadership category, F5, Imperva, and Radware are at the top. Following these top leaders are Google, AWS, and Fastly clustered just below as product leaders closely followed by Check Point.

In the Product Challengers section, Prophaze and Link11 are positioned just below Product Leadership. Rounding out the list of challengers are Wallarm, Cisco, and Qrator Labs.

UBIKA is the only follower in this Product Leadership category.

Product Leaders (in alphabetical order):

- AWS
- Check Point
- F5
- Fastly
- Google
- Imperva
- Radware

Innovation Leadership

Next, we examine innovation in the marketplace. Innovation is, from our perspective, a key capability in all IT market segments. Customers require innovation to meet evolving and even emerging business requirements. Innovation is not about delivering a constant flow of new releases. Rather, innovative companies take a customer-oriented upgrade approach, delivering customer-requested and other cutting-edge features, while maintaining compatibility with previous versions.

This view is mainly based on the evaluation of innovative features, services, and/or technical approaches as defined in the Required Capabilities section. The vertical axis shows the degree of innovation plotted against the combined/overall strength on the horizontal axis. The Innovation Leadership Chart is rectangular and divided into thirds. Innovation Leaders occupy the top section. Challengers are in the center. Followers are in the lower section.

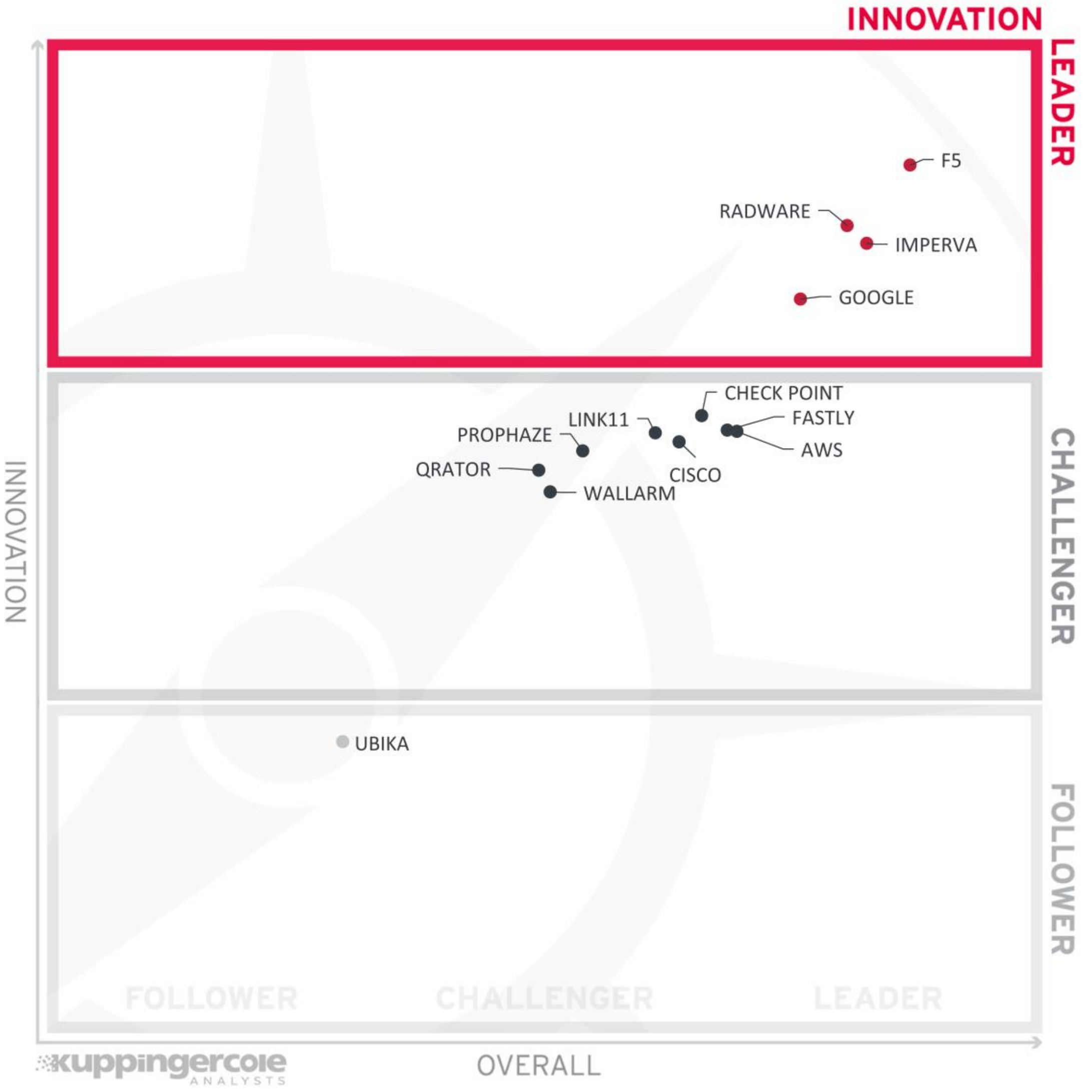


Figure 4: Innovation Leadership in the WAAP market

Innovation Leaders are those vendors that are delivering cutting-edge products, not only in response to customers' requests but also because they are driving the technical changes in the market by anticipating what will be needed in the months and years ahead. There is a correlation between the Overall, Product, and Innovation Leaders, which demonstrates that leadership requires feature-rich products that are looking over the horizon to bring advancements to help their customers.

In the Innovation Leadership category, F5, Radware, Imperva, and Google are recognized as the most innovative vendors.

In the Innovation Challengers section, Check Point, Fastly, AWS, Link11, and Cisco are positioned near the Leadership threshold. Subsequently, Prophaze, Qrator Labs, and Wallarm form a cluster, representing the final Challenger vendors.

UBIKA is the only follower in this Innovation Leadership rating.

Innovation Leaders (in alphabetical order):

- F5
- Google
- Imperva
- Radware

Market Leadership

Finally, we analyze Market Leadership. This is an amalgamation of the number of customers, the geographic distribution of customers, the size of deployments and services, the size and geographic distribution of the partner ecosystem, and the financial health of the participating companies. Market Leadership, from our point of view, requires global reach.

In this chart, the vertical axis shows the market strength plotted against the combined/overall strength on the horizontal axis. The Market Leadership Chart is rectangular and divided into thirds. Market Leaders occupy the top section. Challengers are in the center. Followers are in the lower section.

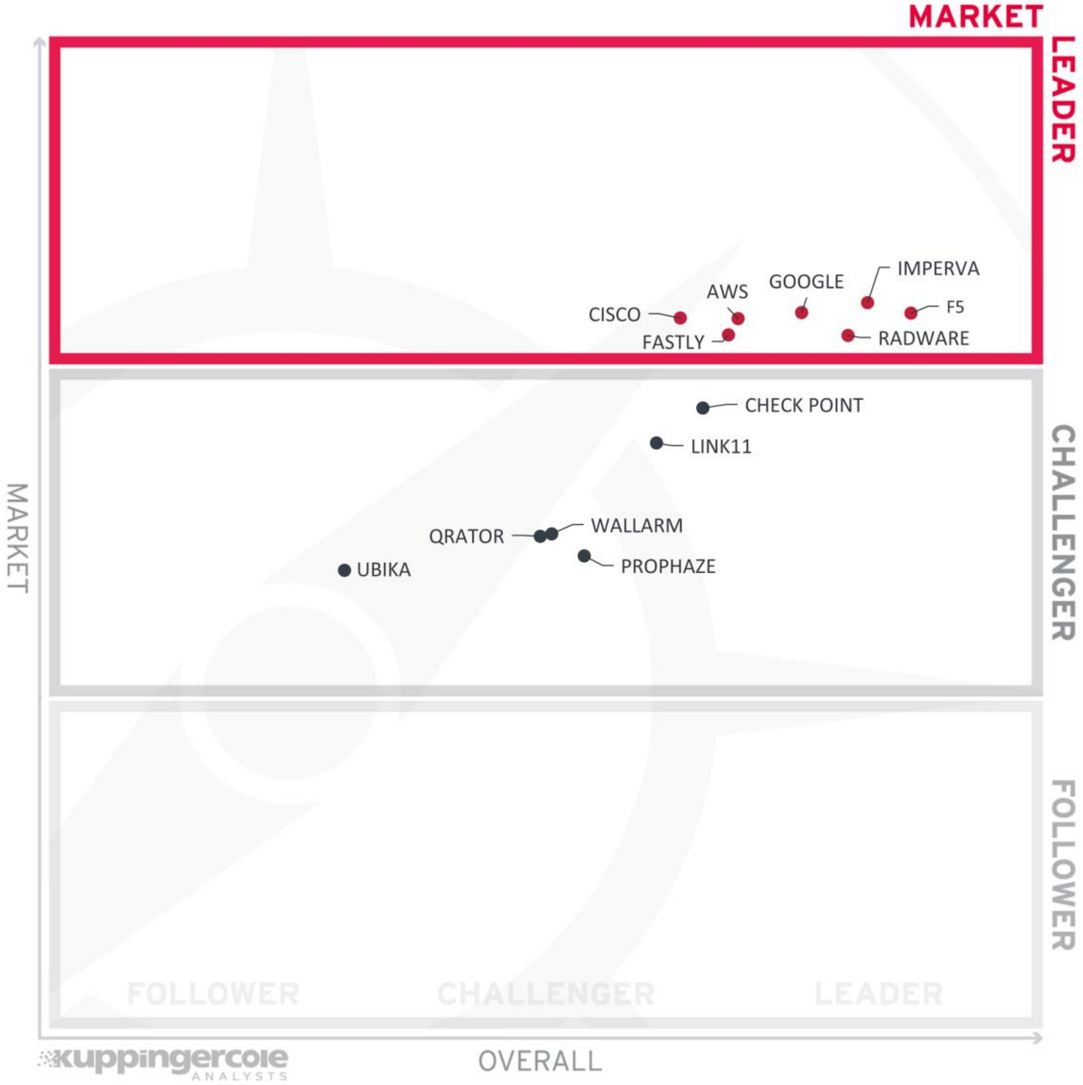


Figure 5: Market Leaders in the WAAP Market

In the Market Leadership category, Imperva, F5, Google, AWS, Cisco, Fastly, and Radware are positioned as the leading vendors.

In the Market Challengers section, Check Point and Link11 are on the verge of becoming market leaders. The list of market challengers is rounded out by Wallarm, Qrator Labs, Prophaze, and UBIKA.

There is no follower in this Market Leadership rating.

Market Leaders (in alphabetical order):

- AWS
- Cisco
- F5
- Fastly
- Google
- Imperva
- Radware

Product/Vendor evaluation

This section contains a quick rating for every product/service we've included in this KuppingerCole Leadership Compass document. For many of the products there are additional KuppingerCole Product Reports and Executive Views available, providing more detailed information.

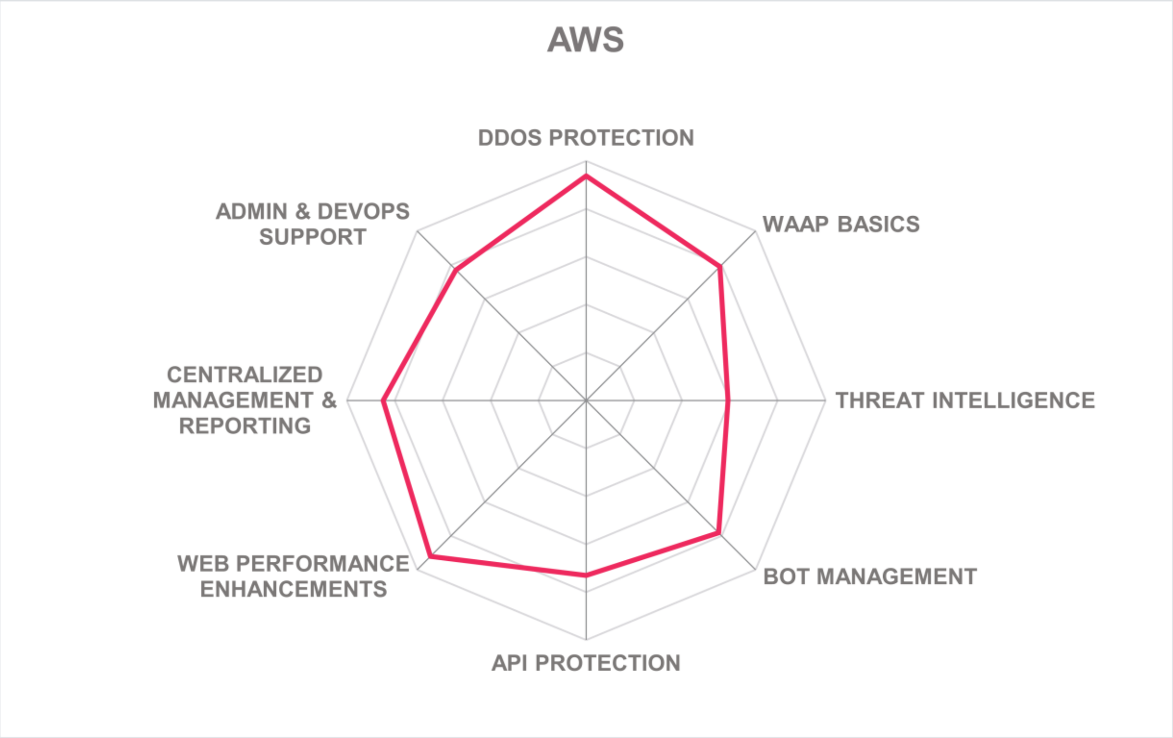
Spider graphs

In addition to the ratings for our standard categories such as Product Leadership and Innovation Leadership, we add a spider chart for every vendor we rate, looking at specific capabilities for the market segment researched in the respective Leadership Compass. For this market segment, we look at the following categories:

- **DDoS Protection:** DDoS is the type of attack that attempts to make an organization's web applications, APIs, or network unavailable for use by legitimate customers. There are many variants of DDoS attacks, but regardless of the method of attack, DDoS protection should be a fundamental capability to consider in any WAAP solution.
- **WAAP Basics:** These cover many of the most common types of protections against web attacks and are often found in the OWASP Top 10 Web Application Security Risks or CWE Top 25.
- **Threat Intelligence:** Leveraging advanced data analytics, threat intelligence feeds, and ML algorithms to enhance the effectiveness of a WAAP platform. By analyzing traffic patterns, user behaviors, and external threat intelligence sources, a WAAP solution can block known attack patterns and adapt to new and evolving threats in real-time, including those targeting API endpoints. Supporting CTI standards and protocols allows WAAP solutions share and receive threat intelligence with the other tools and wider cybersecurity community. This helps security teams to identify new threats faster and respond more effectively.
- **Bot Management:** Bot management addresses how the vendor services aid customers in handling bots. Common options are challenging, redirection, and throttling. Advanced bot management includes the ability to deploy sophisticated proof-of-work and/or user-friendly, unobtrusive challenges that improve transaction security but not at the expense of the user experience. Other bot management techniques include redirecting known or suspected bots, throttling, and enforcing allow- and denylists. Bot detection and management can help prevent automated ATO and New Account Fraud (NAF) attempts.
- **API Protection:** Securing APIs against the attacks listed on the OWASP API Security Top 10 list, as well as API authentication and authorization, validating API calls against API schemas, scanning and/or filtering payload data, and other API-specific capabilities. Modern WAAP solutions are increasingly evaluated based on their depth of API visibility, automatic API discovery, support for schema enforcement, and protection against abuse of exposed APIs. This area is now a central pillar of WAAP functionality due to the rising volume and impact of API-based attacks.

- **Web Performance Enhancements:** Web acceleration and CDN support, geographic regional networks, and capabilities such as HTTP optimization, caching and prefetching, compression, content filtering, etc. Additionally, API traffic management features such as rate limiting, quota enforcement, and caching are now essential for ensuring reliable and secure API delivery.
- **Centralized Management & Reporting:** This includes a centralized location to manage WAAP security policies and rules, monitor availability and performance, handle alerts, run analytics, and enforce governance across both web and API traffic.
- **Admin & DevOps Support:** Available assistance options for administrators and operations teams to support their tools, automation, and third-party integrations. Also evaluated is the vendor’s ability to support developers using the solution’s APIs through documentation, tutorials, tools, knowledgebase, and collaborative support/platforms for developers. This includes support for integrating WAAP functionality into CI/CD pipelines and securing APIs as part of the development lifecycle.

AWS – AWS WAF



Leader in

OVERALL LEADER

PRODUCT LEADER

INNOVATION LEADER

MARKET LEADER

Amazon Web Services, Inc. (AWS) is a multinational cloud service provider headquartered in Seattle, USA. AWS was initially formed as a subsidiary of the American retail giant Amazon.com to consolidate and standardize the computing infrastructure powering Amazon's online business. AWS provides a flexible WAF that can be deployed across various AWS services depending on an organization's business needs. Users can either manage the WAF directly or opt for managed protection via AWS services. AWS WAF offers capabilities to secure both web applications and APIs, including traffic filtering, bot mitigation, DDoS defense, and protections against ATO and fake account creation. It orchestrates with Amazon CloudFront (AWS's CDN), and leverages AWS threat intelligence solution to identify and respond to malicious activity. To expand its capabilities, AWS WAF integrates with complementary solutions such as AWS Shield for DDoS protection and AWS Firewall Manager for centralized rule management across accounts.

AWS WAF is a cloud-native managed service primarily deployed via Amazon CloudFront, API Gateway, application load balancer, and AppSync. Although not natively deployable on-premises, hybrid and multi-cloud scenarios are supported via edge-based deployments. For cloud deployments, it integrates with AWS compute and networking solutions. AWS WAF supports SaaS delivery and can be extended via container services like Elastic Container Service (ECS), Elastic Kubernetes Service (EKS), and AWS Fargate, orchestrated using Kubernetes or native AWS tooling. The solution supports microservices-based development and integrates into DevSecOps pipelines through AWS CloudFormation, AWS CDK, and Terraform. Both Command Line Interface (CLI) access and Software Development Kits (SDKs) across languages like Python, Java, and Go are available. It supports API standards such as REST, JSON, and GraphQL. AWS WAF is compliant with major regulations such as GDPR and HIPAA, standards like PCI DSS, ISO 27001, FIPS 140-2, and NIST 800-171, frameworks like US FedRAMP, and SOC 1/2/3 certified.

AWS Shield Standard offers Layer 3 (L3) and Layer 4 (L4) mitigation by default, while AWS Shield Advanced provides L7 protections. Customers subscribed to Shield Advanced also gain access to the AWS Shield Response Team (SRT), which assists with real-time incident mitigation. AWS WAF does not handle functions like API authentication, API routing, API response caching, and API key mechanisms directly. These are done by AWS API Gateway or upstream solutions. AWS WAF integrates with AWS API Gateway and AppSync to enforce API security policies, including rate limiting, token-based authentication, API key management, and allow/block lists.

AWS WAF provides preconfigured managed rule groups from AWS and third-party providers via the AWS Marketplace. It offers built-in protection against the OWASP Top 10 threats and supports importing external signatures or custom rule definitions. AWS WAF orchestrates with Amazon GuardDuty to ingest threat intelligence and apply it to web access control lists (ACLs). Managed rule groups also support use cases such as account takeover prevention, account creation fraud prevention, and advanced bot detection through the bot control package. AWS applies both supervised and unsupervised ML algorithms to enhance detection accuracy and reduce false positives.

AWS WAF’s managed rules offer bot detection and mitigation capabilities, targeting basic bots, sophisticated bots, ATO attempts, and fraudulent account creations. These functionalities extend to common bots with self-identifying signatures and targeted bots with application-specific signatures. Passive biometrics and ML algorithms are used for bot detection. ML algorithms help detect credential stuffing, scraping, and reconnaissance activity. ML methods are also employed to block known bot attacks and identify volumetric anomalies based on suspicion scores. It deploys CAPTCHA challenges and silent challenges for verification processes that run in the background. CAPTCHA and silent challenge features verify user authenticity, while Bot Control allows rule-based responses such as, allow, block, and rate-limit, based on bot category (e.g., crawler, scanner, scraper). AWS also uses an IP reputation list to help assess bot risk.

For vulnerability remediation, AWS WAF relies on orchestration with other AWS and partner solutions. AWS IAM ensures secure access and policy enforcement. Meanwhile, AWS CloudTrail supports audit logging. Third-party integrations through AWS Marketplace support virtual patching and vulnerability scanning. While AWS WAF does not natively perform vulnerability assessments or support CTI standards, it does offer extensive interoperability via APIs.

Organizations seeking a global WAAP vendor with an engine that covers most WAAP use cases and that prioritize scalability and orchestration within a cloud-native ecosystem should consider AWS. This is especially true for organizations that are already invested in the AWS ecosystem and require integration with AWS solutions to achieve comprehensive cybersecurity.

Strengths

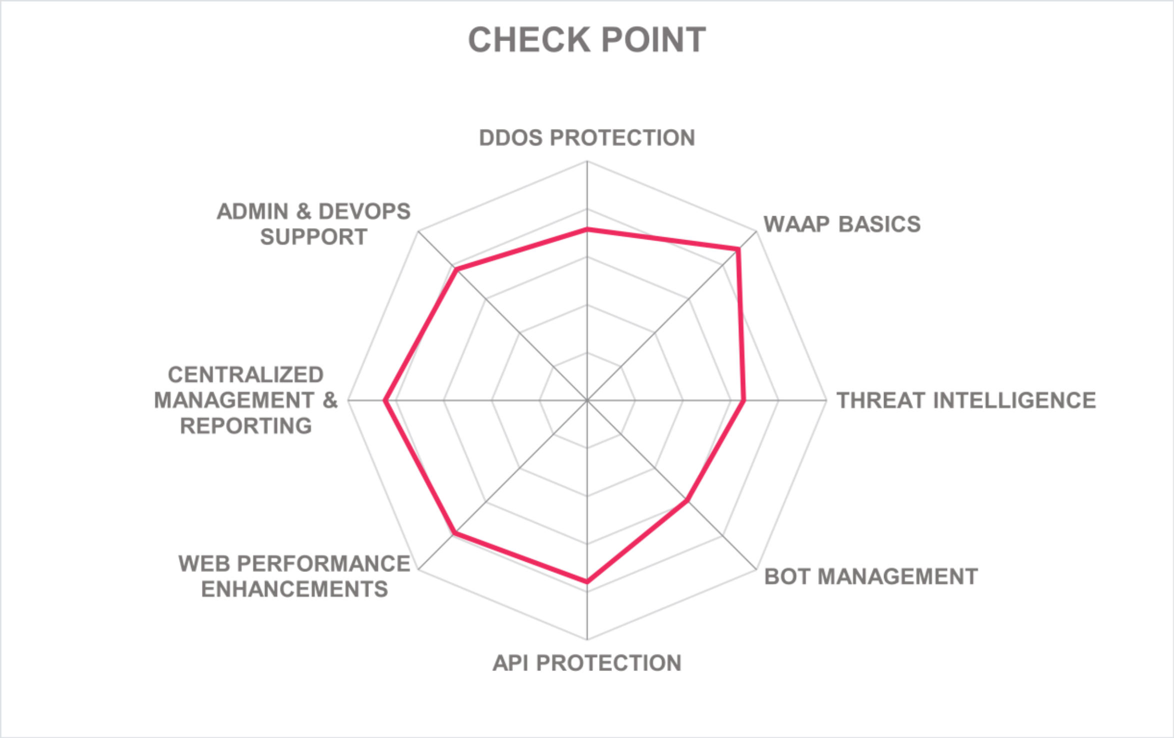
- Excellent integration capabilities
- Excellent global reach and partner ecosystem
- Comprehensive compliance support
- Global PoPs are scrubbing center infrastructure
- Easy access to integration with other tools through the AWS Marketplace
- Managed Rules provide a quick start with pre-configured application protection rules
- Custom rule definitions and external signature imports are supported
- Additional visualization and analytics capabilities are accessible through other AWS solutions, but these features come with additional charges
- Good logging capabilities, with easy storage and sharing options within the AWS environment
  PBAC is supported for delegated administration

Challenges

- In order to obtain full-spectrum WAAP coverage, additional licenses are required
- Not available on-premises
- It does not offer vulnerability assessments
- No support for CTI standards and protocols

Checkpoint – CloudGuard

CHECK POINT™



Leader in

OVERALL LEADER

PRODUCT LEADER

INNOVATION LEADER

MARKET LEADER

Check Point, established in 1993 and headquartered in Tel Aviv, Israel, provides WAAP through its CloudGuard platform. CloudGuard offers WAF, API protection, Bot Management, DDoS Protection, sensitive data protection, and threat prevention features within a unified platform. The solution also provide protection against zero-day, Server-Side Request Forgery (SSRF), XSS, and credential-stuffing attacks.

CloudGuard supports deployment in hybrid environments and Kubernetes clusters. The solution can be delivered as a managed SaaS or deployed via Docker containers and Helm charts on Kubernetes. The platform supports integrations with third-party threat intelligence, DLP, DevSecOps, and CDN platforms natively. Further integrations are facilitated by REST and GraphQL protocols. CloudGuard also orchestrates effectively with other Check Point solutions, such as Check Point XDR. Check Point is an ISO 27001 and SOC 2 Type 2 certified vendor, and complies with GDPR and HIPAA regulations, and PCI-DSS standard.

DDoS protection is integrated at both the edge and L7. The solution leverages real-time threat intelligence, rate-based blocking, behavioral analysis, and request scoring to prevent L3, L4, and L7 DDoS threats. DDoS protection is active by default and can be fine-tuned using policy templates or dynamic thresholds. The solution also integrates with third-party CDN and cloud load balancing services to absorb L3 and L4 attacks.

CloudGuard WAF protects APIs and web applications within a unified platform, available in both SaaS and IaaS delivery models. The negative model utilizes a two-layer AI approach: an attack indicator engine that detects attack patterns without using traditional signatures, and a context analysis engine that evaluates user behavior, traffic patterns, application logic, and trusted user status. The positive model is enforced through automated API discovery and schema validation and restricts traffic to known and validated patterns. The solution provide protection against SQL and code injection, malicious file uploads, and XSS. It also supports virtual patching and contextual inspection of HTTP traffic.

The premium offering includes continuous API discovery and protection capabilities that use ML detection mechanisms to analyze live traffic and identify all exposed endpoints. The solution automatically generates API schemas by capturing parameters and request structures and applies rate-limiting to control request volumes. It integrates with API gateways and proxies such as Kong and Envoy in Kubernetes. In addition, access control and threat classification are applied to defend against API abuse, credential stuffing, and business logic attacks.

CloudGuard detects and mitigates bot threats without relying on static activity signatures. Bot detection is based on ML and behavioral analysis, which assess request patterns, IP reputation, and interaction characteristics to distinguish malicious bots from legitimate traffic. Rather than matching known indicators, the solution analyzes traffic to identify anomalies to reduce dependency on frequent signature updates. Risk-based challenges, such as CAPTCHA and reCAPTCHA, are dynamically triggered in response to suspicious behavior, including scraping, credential abuse, or automated form submissions.

CloudGuard orchestrates with Check Point's ThreatCloud AI platform, which delivers real-time threat intelligence based on numerous sensors globally. The solution analyzes attack patterns, indicators of compromise (IoC), and global threat activity to inform its prevention capabilities. This intelligence is applied through the dual-layer AI engines that were previously explained in this paper. The intelligence feed enriches application events with reputation scores and threat classifications. Administrators can also import custom SNORT or Intrusion Prevention System (IPS) signatures to align with third-party threat feeds.

The platform scans and automatically patches Common Vulnerabilities and Exposures (CVEs) natively, and it can proactively block exploit attempts through its threat prevention engine. In terms of visibility, CloudGuard logs and audits security events with granularity across request types, origins, and traffic behaviours. Logs can be forwarded to external SIEM platforms, and administrative actions are auditable. While not specifically designed for DLP, the platform supports field redaction in logs to prevent sensitive information from being exposed during analysis.

Check Point's CloudGuard is a well-established product in the WAAP market, particularly in Europe and the Middle East. Its flexible licensing options and deployment models make it suitable for organizations of all sizes. CloudGuard also benefits from Check Point’s extensive partner network and integration with the Infinity architecture.

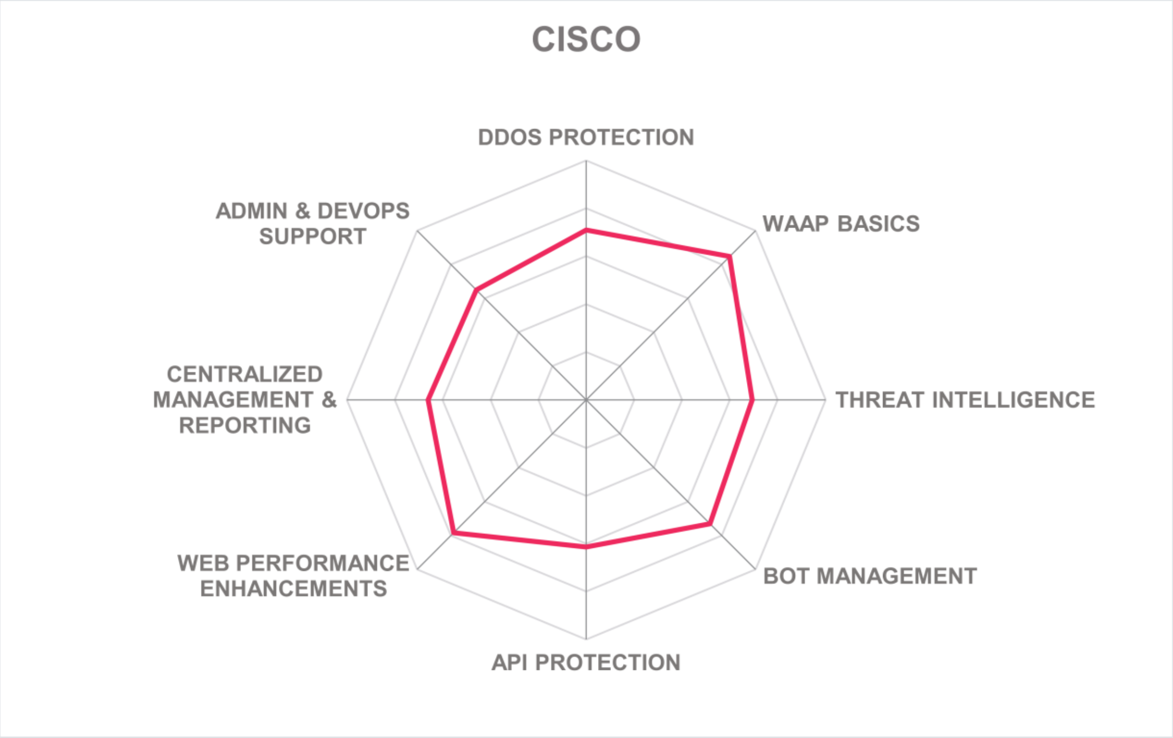
Strengths

- Strong partner ecosystem
- Charter Member of Cyber Threat Alliance
- Integrates with Check Point XDR and ThreatCloud AI for orchestrating threat detection
- Custom SNORT and IPS signatures are supported for third-party threat feeds
- Automatic CVE scanning and virtual patching for exploit prevention
- Access control and threat classification are applied to prevent API abuse
- AI and ML algorithms are effectively utilized for threat intelligence and bot management.

Challenges

- Dashboards are not customizable and could be more user friendly
- Does not use passive biometrics for bot detection
- Some API protection features are not supported in the standard plan
- Data masking capabilities are limited to field redaction in logs
- Reporting capabilities are limited

Cisco – Cisco WAAP



Cisco, founded in 1984 and based in San Jose, California, offers Cloud WAAP, in partnership with Radware, as part of its Secure Application Security portfolio. The WAAP solution includes the Cisco Secure Web Application Firewall, Cloud Bot Manager, API protection module, Layer 7 DDoS protection, DLP, and Cisco Secure Access client-side protection.

Cisco Cloud WAAP can be set up as SaaS sensors, Kubernetes-based WAF nodes, or on-premises hardware and virtual appliances. Supported by Radware ERT, it is also available as a fully managed service. It has dedicated connectors for major public cloud providers like AWS, Azure, and GCP. The platform supports the REST API protocol for third-party integrations and can be orchestrated with other Cisco solutions when a full-spectrum WAAP is needed. Cisco support compliance with regulations like NIS2, GDPR, HIPAA, and DORA, and standards like PCI DSS through built-in security and audit controls. While SDKs are not currently available, configuration and policy management can be done through a centralized web interface.

Cisco's Cloud WAAP provide protection against L7 DDoS attacks, including HTTP floods, bot-driven attacks, and form-based abuse. It uses behavioral analysis and ML for mitigation.

L3 and L4 DDoS mitigation is available only through a separate Cisco Secure DDoS Protection add-on, not included in the core WAAP package. CDN integration is part of the unified WAAP experience, which can be accessed via a centralized management console. Cisco operates a network of PoPs and scrubbing centers for its DDoS and secure WAAP platform. These data centers are located in major regions around the world. Cisco routes traffic through Anycast to the nearest scrubbing PoP when attack thresholds are reached. This infrastructure helps mitigate both L3, 4, and L7 attacks directly at the edge, without requiring redirection to core systems.

The web application firewall combines positive and negative security models to guard against OWASP Top 10 web and API vulnerabilities, zero-day exploits, and client-side threats. The solution employs signature and behavior-based techniques. The Advantage and Premier plans include advanced detection and response capabilities, such as path-specific enforcement mechanisms and AI-driven correlation logic for more accurate threat analysis.

API protection in Cisco WAAP includes automatic discovery of exposed endpoints, schema validation, and OpenAPI integration. Policies can be created dynamically based on observed traffic and applied in real-time. The solution maps the API attack surface through automated discovery and creates custom policies to block API attacks in real time. Advanced API protection capabilities are included in the higher tiers. These tiers offer increased automation and more granular precision in detecting and blocking malicious API requests.

Cisco WAAP’s threat intelligence is powered by Cisco Talos, which provides real-time updates sourced globally to inform security policies. Higher tier users are given access to more sophisticated intelligence feeds. These plans also offer support from Cisco’s emergency response experts, who help refine threat detection rules and conduct proactive threat hunting.

Cisco's bot management uses a multi-layered approach. It includes behavioral analytics, JavaScript-based challenges, mobile client verification, and unique methods like blockchain-backed crypto challenges to identify and reduce malicious bot traffic. Basic features are available in the standard plan. More advanced bot protection features, such as intent-based analysis and greater customization options, are only available in the higher tiers. The platform’s vulnerability management offers features like automated virtual patching and real-time alerts for known vulnerabilities. DLP features mask or block sensitive data to prevent exposure through web application attacks.

Cisco Cloud WAAP is a good option for mid-sized to large enterprises that need scalable and integrated WAAP. It supports API-first architectures and centralized control models. The solution is especially suitable for organizations that require all core WAAP capabilities in a regulated environment.

Strengths

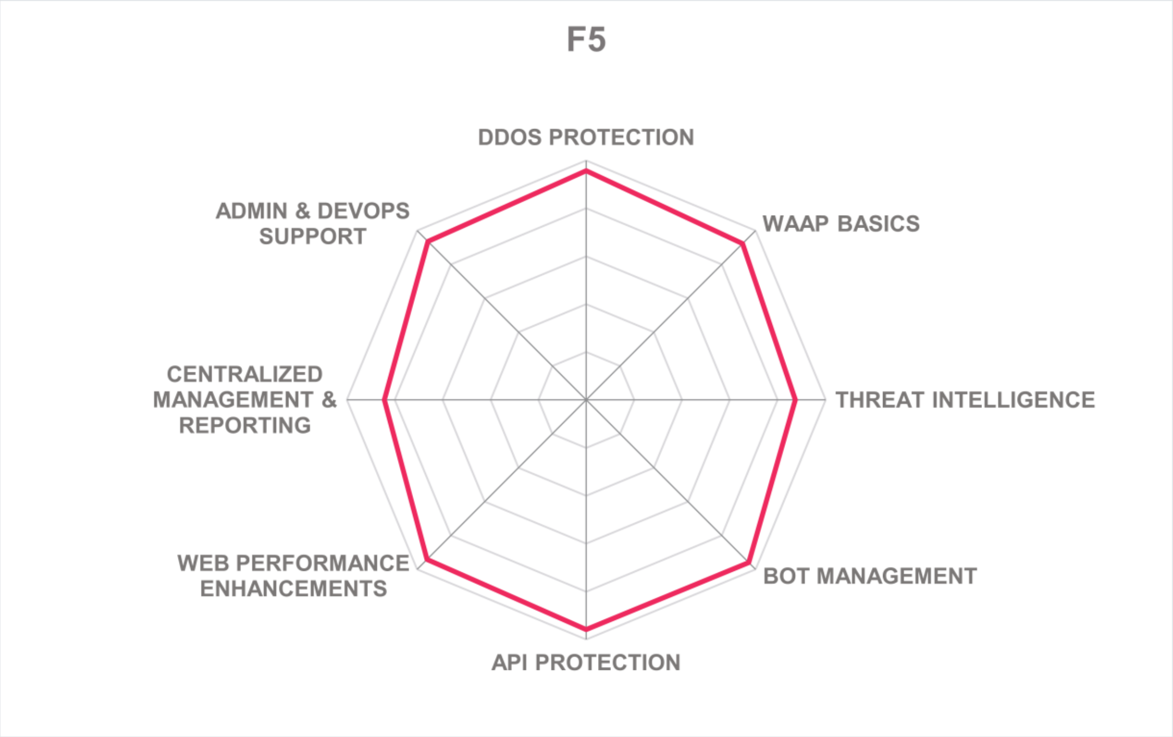
- Charter Member of Cyber Threat Alliance
- Excellent global reach and partner ecosystem
- Comprehensive compliance support

- Supports innovative bot challenging methods, such as blockchain-backed crypto challenges
- Automates complex tasks like policy tuning, API discovery, event analytics, and supply chain mapping
- Radware's ERT provides customers with a fully managed service
- API attack surface mapping is supported

Challenges

- Third-party attack signatures and rule sets are not supported
- No CDN capability out-of-the-box
- Advanced API protection is not included in the standard plan
- No support for mobile SDKs
- L3 and L4 DDoS mitigation requires a separate license
- Limited reporting capabilities

F5 – F5 WAAP



Leader in

OVERALL LEADER | PRODUCT LEADER | INNOVATION LEADER | MARKET LEADER

Founded in 1996 and headquartered in Seattle, Washington, F5 is a publicly traded company that delivers application security and delivery solutions. The company maintains a strong customer base among large enterprises across North America and globally. F5 is recognized for its mature suite of application-centric technologies. In addition to standard WAF capabilities, the current WAAP portfolio incorporates Secure DNS, Client-Side Defense, Web Application Scanning, and an AI-assisted operations interface that provides actionable insights and facilitates remediation efforts. These features enhance F5's existing security functions, which already include API protection, DDoS mitigation, bot management, CDN, threat intelligence, fraud detection, virtual patching, and DLP.

F5 offers deployment flexibility across various environments using a common WAAP engine, whether through SaaS or managed service offerings. WAAP can be deployed in cloud, on-premises, containerized, serverless, and VM-based environments. It supports integration with container platforms such as Docker, Red Hat OpenShift, and Rancher. F5 enforces consistent policies across hardware, software, SaaS, and managed service formats which reduce complexity in multi-cloud and hybrid scenarios.

All the F5 WAAP solutions' capabilities are available via API. The solutions support REST, SOAP, gRPC, and GraphQL API protocols. All F5 functions are accessible through the CLI, and the solution supports mobile SDKs and JavaScript. F5 integrates with most essential third-party solutions such as Splunk, Sumo Logic, Qualys, Rapid7, TrendMicro, CrowdStrike, Microsoft Sentinel, Palo Alto Networks, Cisco, Okta, ServiceNow, and Terraform. Built-in compliance templates and reporting help organizations show whether they meet industry regulations like HIPAA, DORA, standards, such as PCI-DSS, and frameworks like BSI C5. This can be done without needing separate appliances or code changes. F5 is also a SOC 2 Type 2 certified vendor.

F5 provides DDoS protection as a managed service through its distributed mitigation infrastructure. The solution defends against L3 and L4 attacks as well as more sophisticated L7 threats. It leverages network and application-layer mitigation techniques to limit disruption while maintaining application availability. Supported by ML-powered detection models and adaptive signatures, application-layer DoS protection dynamically adjusts based on system stress and behavioral indicators.

F5 WAAP implements sophisticated API security measures to protect against the OWASP Top 10 for APIs and includes automatic API discovery and API testing functionalities. The platform can be integrated with F5 NGINX to provide API gateway capabilities. It supports essential API security features like schema validation, rate limiting, allow-listing, and API routing. Additionally, API key mechanisms are used to block anonymous traffic, manage quotas, and authorize access.

Basic WAF capabilities include protection against common application attacks, such as OWASP Top 10 and SQL/PHP protection for both applications and data as well as OWASP Top 10 for LLM Applications. F5 WAAP also defends against known vulnerabilities, zero-day attacks, and cross-site scripting (XSS). F5 WAAP solutions can employ either the negative or positive security model or a hybrid approach that combines both. In addition to signature and rule-based approaches, F5 WAAP uses behavioral analytics and probabilistic ML tuning to identify and mitigate attacks in the negative security model.

For the positive model, the platform can create custom signatures and rules, as well as utilize third-party ones. The solution comes with advanced security threat tools that provide predictive behavioral analysis and threat intelligence. It leverages risk-based policies across multiple security services and provides insightful analysis of risks associated with multi-cloud applications. F5's behavioral WAAP uses AI and ML algorithms to mitigate risks by tracking user behavior, detecting malicious activities, and assigning risk scores to them. F5 has recently improved its ADSP platform with Agentic AI through its integration with Fletch technologies. Agentic AI delivers contextual insights and practical suggestions, like policy changes or automated blocking actions. This integration offers better automation and context-awareness for threat management. F5 can also integrate with well-known threat intelligence feeds and use multiple sources. However, the platform does not adhere to CTI standards and protocols for threat sharing purposes.

Bot management capabilities are included in the base WAAP offering, with more advanced detection and mitigation features available through upgraded tiers. The solution employs activity signatures and ML algorithms, such as anomaly clustering, to identify bots. The F5 platform supports passive biometrics using behavioral analysis. It looks at factors like typing patterns, mouse movements, and device characteristics to identify bots and fraudulent activity. The bot challenge methods include CAPTCHA, JS challenges, and temporary blocking. These methods are configurable by customers. F5 WAAP offers customizable allow-listing and deny-listing capabilities. The enhanced bot module also leverages advanced signal collection in browsers and mobile SDKs to detect automation frameworks and human-like emulation.

F5 WAAP is also capable of identifying signs of web application misconfigurations by monitoring server responses and application latency. Secure DNS, Client-Side Defense, and Web App Scanning extend this visibility to DNS-layer exploits, in-browser JavaScript attacks and exposed Internet-facing assets, respectively. F5 WAAP comes with built-in vulnerability scanners and can integrate with other popular vulnerability scanners. The system can automatically identify sensitive data and replace it with asterisks in the logs. Credential protections are available with application-level encryption. Mitigation of credential cracking and stuffing attacks is achieved through F5 Bot Defense.

F5 WAAP is an excellent option for large enterprises looking for a WAAP solution. Its versatility across deployment models and integration with major platforms make it a strong candidate for enterprises with complex, multi-cloud environments. However, the solution may be too sophisticated for small organizations.

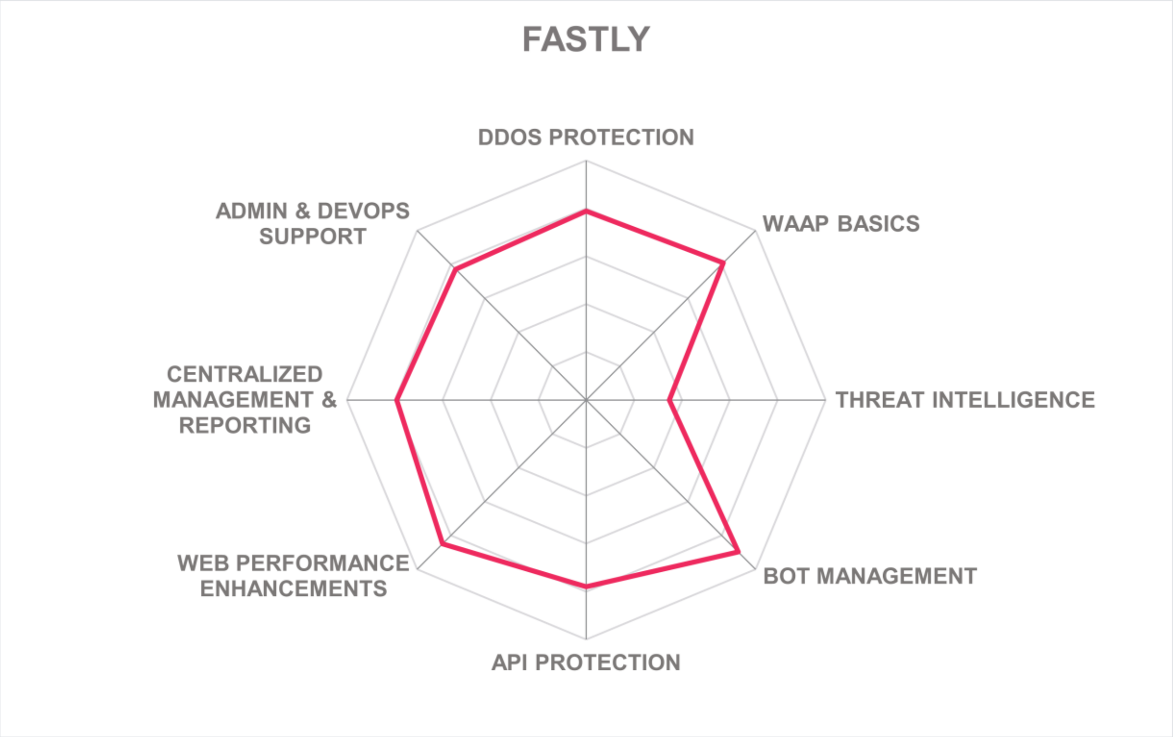
Strengths

- Excellent partner ecosystem
- Support for an extensive range of API protocols
- Strong integration capabilities with third-party solutions
- Comprehensive protection for mobile apps and platforms
- Effective data masking techniques to protect sensitive data
- Support for a wide range of regulatory compliance requirements and standards
- SOC teams provide 24/7 support to customers for incident response and remediation
- Leverages threat intelligence feeds from trusted sources in conjunction with its proprietary threat intelligence tools
- Agentic AI provides automated, policy recommendations and blocking actions
- Protection against OWASP Top 10 for Large Language Model (LLM) Applications
- Policy-based risk scorings are available
- Session recording to track and analyze user sessions for security and troubleshooting purposes
- ABAC and PBAC are supported for delegated administration

Challenges

- More sophisticated techniques could improve bot challenge methods
- No support for CTI standards and protocols
- Advanced bot detection and mitigation features are only available in upgraded tiers
- Dashboards are not customizable

Fastly – Application Security Solutions



Leader in

OVERALL LEADER

PRODUCT LEADER

INNOVATION LEADER

MARKET LEADER

Fastly, founded in 2011 and based in San Francisco, California, offers Next-Gen WAF, Bot Management, DDoS Protection, API Security, Client-Side Protection, and AI Bot Management modules in a unified platform. The platform also provides protection for SQL injection attacks, automated API abuse, data skimming, and new zero-day exploits.

The Fastly platform supports public cloud, private cloud, multi-cloud, hybrid cloud, and on-premises deployment models. Fastly can be deployed as SaaS, virtual appliance, container image for Docker and Kubernetes, or serverless function on Fastly Compute. CLI and SDKs are also supported. The third-party integrations are facilitated through REST, SOAP, XML, and gRPC protocols. Out-of-the-box integrations include tools like Splunk, Datadog, Cisco SecureX, Kong, and Terraform. Fastly is an ISO 27001 and SOC Type 2 certified vendor and complies with GDPR, and HIPAA regulations, as well as PCI-DSS standard. It also provides documentation on these regulations and standards via a developer portal.

Fastly’s Attribute Unmasking technology analyzes L3, L4, and L7 traffic in real time. It isolates attacker fingerprints and mitigates various DDoS attack types. Mitigation occurs at the nearest PoP, which helps prevent latency issues that typically arise from off-path scrubbing centers. Their PoPs are located in all major regions around the world.

The Fastly Next-Gen WAF employs SmartParse, a Natural Language Processing (NLP) based detection engine, lexical analysis, a context-aware detection engine that avoids signature tuning and reduces false positive instead of relying on traditional reg-exp signatures. It provides protection against OWASP Top 10 web attacks and advanced threats such as ATO, malicious bots, and API abuse.

API discovery and protection features are offered out-of-the-box. The solution support integration with service mesh and API gateway technologies such as Kong and Envoy. OpenAPI schema validation is executed by comparing incoming API requests against specifications provided by users. When deviations are detected, the system generates an alert. The solution also applies rate limiting, enforces request quotas, and supports rule-based allow lists to restrict access to approved behaviors.

The WAF module also includes the Network Learning Exchange (NLX), which is a threat intelligence feed based on IP reputation that is shared across Fastly’s customer network. The threat intel data is sourced from numerous daily requests passing through the edge. Administrators can supplement the threat intel feeds with external sources by using webhook or API connectors. CTI sharing standards such as STIX are not yet supported.

Bot Management combines server-side request analysis with a lightweight JavaScript snippet for client-side monitoring. The system checks behavioral patterns, browser capabilities, and Apple’s Private Access Tokens (PATs) to accurately classify automation. Dynamic Challenges apply the least resistance needed to validate traffic, using JavaScript proof-of-work, non-interactive puzzles, or CAPTCHA as risk levels increase. Security teams can allow benign bots, mislead scraping tools with different responses, or redirect unwanted automation to honeypots.

Fastly Next-Gen WAF also helps customers with vulnerability mitigation, which finds malicious payloads and applies virtual patches without needing manual signature adjustments. DLP mechanisms remove sensitive headers, parameters, and patterns, including PII and financial data, before logs are sent to external storage. Fastly’s CDN uses an edge-first architecture to accelerate the delivery of both static and dynamic content. It supports HTTP/3 and TLS 1.3, as well as instant cache purging and origin shielding, which reduce origin load for improving performance. Transmission Control Protocol (TCP) multiplexing and optimized routing allow site acceleration. Together with DDoS protection, edge compute functions support secure content delivery.

Fastly WAAP is a solid solution in the WAAP market. Its modular structure and licensing options make it suitable for organizations of all sizes. Fastly maintains a strong market presence in the United States, where it generates the majority of its revenue, and demonstrates growing traction in the Asia-Pacific and European regions.

Strengths

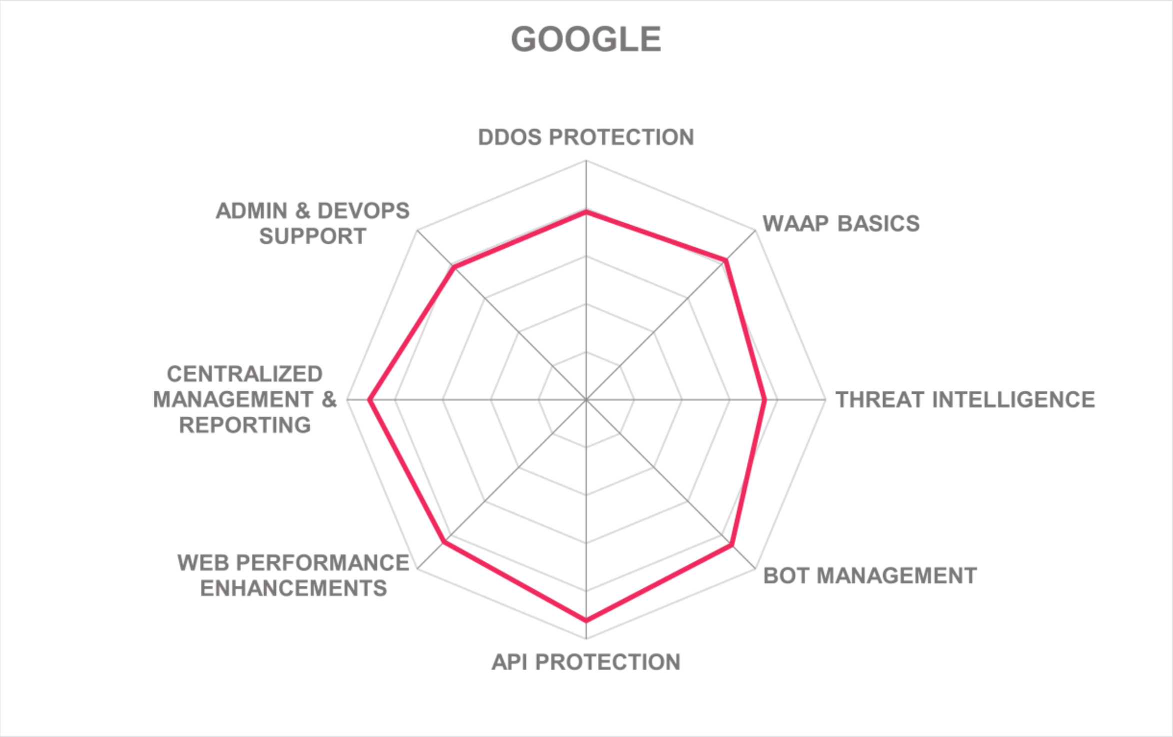
- Support for major API protocols
- Solid bot management capabilities
- Dynamic Challenges are applied as risk levels increase
- Attribute Unmasking technology mitigates DDoS attacks at edge PoPs
- SmartParse lexical analysis reduces false positives, avoids manual signature tuning, and enables virtual patching for malicious payloads
- Data masking is applied to sensitive information before log export.
- One of the highest global edge network capacity in the WAAP market
- Users can configure and choose preferred bot challenge methods based on their risk and usability preferences

Challenges

- No support for CTI standards and protocols
- Custom API protection policies rely on user-supplied OpenAPI specs
- API authentication and routing are not supported
- Limited CTI capabilities
- Limited use of AI and ML algorithms for threat detection
- Lacks capabilities for vulnerability scanning and remediation

Google – Google Cloud WAAP

Google Cloud



Leader in

OVERALL LEADER · PRODUCT LEADER · INNOVATION LEADER · MARKET LEADER

Google, founded in 1998 and based in Mountain View, California, offers WAAP through Google Cloud Security. The solution combines Google Cloud Armor for WAF protection and DDoS mitigation, Apigee and Advanced API Security for managing and protecting APIs, and reCAPTCHA for bot management.

Google Cloud WAAP supports public cloud, hybrid, and on-premises deployments by integrating Cloud Armor with external HTTP(S), TCP proxy, and SSL proxy load balancers. Apigee operates as a managed SaaS or as a hybrid deployment on Google Kubernetes Engine or other supported platforms. The solution supports REST APIs and Webhooks for integration with third-party solutions. Google Cloud is an ISO 27001, and SOC 1/2/3 certified vendor and complies with the majority of the regulations and standards, such as PCI-DSS, HIPAA, NIS2, and GDPR.

In Cloud Armor, DDoS protection starts with automatically activated L3 and L4 defenses for external load-balanced services. Customers who license the Enterprise tier receive advanced network defense that analyzes telemetry and blocks protocol-based floods before they reach the origin. Adaptive Protection, an ML-powered capability, observes normal application traffic and creates suggested policies that stop L7 DoS attempts such as HTTP floods and slow-rate attacks. Rate limiting is provided to control high volumes of requests that could overwhelm systems and deny access to legitimate users.

Cloud Armor uses predefined WAAP rules from the OWASP Top 10 list to block attacks like SQL injection and XSS. Administrators can create custom policies in Common Expression Language (CEL) and test them in preview mode to assess possible effects before enforcing block actions. Rules can refer to attributes like IP address ranges, geolocation, URL path, or request headers.

Apigee provides API gateway and advanced API security and governance capabilities including request validation of OpenAPI definitions to validate requests, authorization and enforce authentication, quota management, and Spike arrest policies to control traffic bursts. API schema validation blocks malformed or malicious payloads, while analytics measure risks and flag suspicious patterns. Apigee Advanced API Security provides API security posture management and protects APIs. Its capabilities include shadow API discovery, which uses an agentless approach to surface API observations on Google Cloud load balancers and compare them to documented API endpoints in Apigee’s API catalog. The platform also integrates natively with Apigee’s runtime to detect and block suspicious traffic and performs dynamic security posture checks for deployed API proxies to prevent configuration drift.

Google Cloud WAAP's threat intelligence relies on Google’s global infrastructure and internal analysis processes. Adaptive Protection creates ML-based signatures in real time, and Cloud Armor updates policies to address new threats. The platform does not support any CTI protocols and standards.

Bot management combines reCAPTCHA risk scoring with Cloud Armor policies. Each interaction in the traffic is evaluated, and low-risk traffic proceeds without interruption. Requests that do not meet set criteria trigger CAPTCHA challenges or policy-driven blocks. Enterprise tier customers can create specific rules that merge bot signals with other request attributes to improve mitigation strategies. JavaScript tags from reCAPTCHA can provide client-side risk scorings. reCAPTCHA also uses an invisible score-based detection system to distinguish between legitimate users and bots.

Virtual patching is enforced through firewall rules. Administrators receive real-time alerts in Cloud Monitoring and detailed event logs in Cloud Logging. Security Command Center consolidates findings for compliance reporting and investigations. Google Cloud CDN can be placed in front of WAAP-protected services to speed up delivery while keeping security measures in place.

Google Cloud WAAP is a good and innovative alternative for organizations of all sizes that already use Google Cloud or hybrid environments in their operations. Organizations in the finance, healthcare, and retail sectors can benefit from Google’s compliance support and extensive pre- and after-sales services.

Strengths

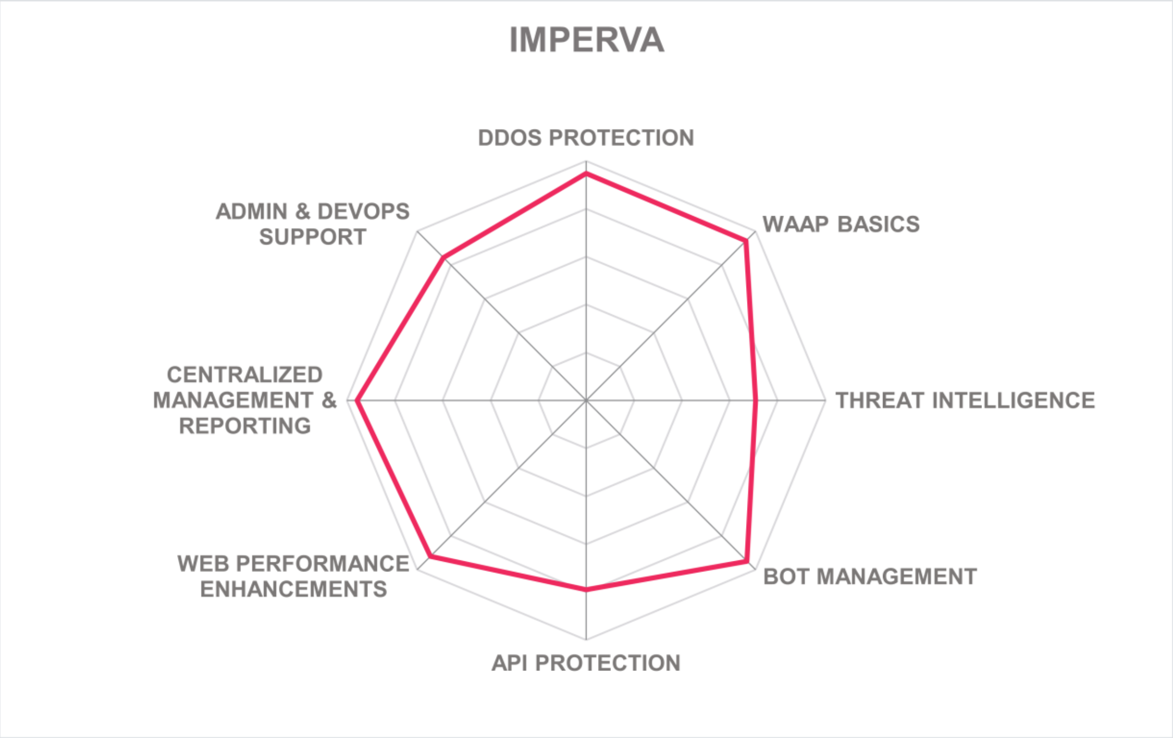
- Excellent global reach and partner ecosystem
- Well-integrated into the broader Google Cloud ecosystem
- Strong API protection and discovery capabilities
- Bot and client-side risk scoring are provided
- Security Command Center supports compliance reporting and investigations
- Cloud Monitoring dashboard highlights a clear overview of metrics
- Gemini Code Assist facilitates API Management and centralized governance by leveraging enterprise context such as API hub assets, security schemas, and patterns to generate and iterate compliant API specifications
- Provides risk scores for each API proxy to keep them secured and compliant with organizational API policies

Challenges

- Third-party attack signatures and rule sets are not supported
- No support for CTI standards and protocols
- Advanced DDoS protection features are not included in the standard plan
- Bot mitigation depends heavily on reCAPTCHA
- Custom rule creation requires familiarity with CEL

Imperva – Application Security

imperva
a Thales company



Leader in OVERALL LEADER, PRODUCT LEADER, INNOVATION LEADER, MARKET LEADER

Imperva, a cybersecurity solution company headquartered in San Mateo, California, began as a provider of web application firewalls in 2002 and has since broadened its portfolio. In December 2023, Imperva was acquired by Thales, a French multinational company serving various sectors including cybersecurity and identity management. Imperva delivers a unified Application Security platform that includes Cloud WAF, Gateway WAF, Elastic WAF for containerized environments, bot protection, API security, client-side protection, attack analytics, and edge services such as DDoS, DNS protection, and CDN.

Their "deploy anywhere" strategy supports on-premises appliances, virtual appliances, SaaS, and the new Elastic WAF. This Kubernetes-native option brings Imperva Cloud WAF enforcement closer to modern microservices. Elastic WAF works with any CDN and any cloud. It is managed centrally from the Cloud Security Console, and CLI automation is also available. A mobile Android and iOS SDK is provided with Advanced Bot Protection. This function enables in-app telemetry for bot detection. REST API management is fully supported. The solution integrates with third-party solutions like QRadar, LogRhythm, Splunk, CrowdStrike, Rapid7, Palo Alto Networks, Qualys, and Terraform. The company holds ISO 27001 and SOC 2 certifications, and complies with PCI-DSS standards.

Imperva delivers multi-layer DDoS mitigation through its global PoP network, protecting L3, L4, and L7 with high bandwidth and low latency. Flow monitoring, network cleaning, and application-level strategies reduce collateral impact of DDoS attacks.

API protection is available as an add-on or as a standalone solution. It provides unified API discovery, risk assessment, and mitigation in one console. The solution integrates with API gateways like Kong, MuleSoft, Azure APIM, Apigee, and F5. Imperva offers automated API discovery for specific websites. It supports real-time inventory updates and schema validation using OpenAPI definitions. The platform allows policy configuration at the API group level. It features data classification for sensitive and personally identifiable information (PII), adjustable authentication and exposure settings, and detection of Broken Object Level Authorization (BOLA) risks. Users can access API endpoint details, including requests, responses, specifications, and related risks, through the management console.

Imperva protects against OWASP Automated Threats and API Top 10 attacks employing both positive and negative security models. ML analytics and the Imperva Threat Research feed continuously refine detection rules. The platform can utilize third-party rules. Imperva can also utilize threat intelligence feeds from multiple sources. Both supervised and unsupervised ML algorithms are used to detect anomalies. The solution does not support any CTI standards and protocols.

Advanced Bot Protection integrates with Cloud WAF or can be deployed via standalone connectors for AWS Lambda@Edge, Cloudflare, Fastly, F5, and NGINX. The platform can detect bots and analyze user behavior using high-definition fingerprinting, biometric-style behavioral analysis, and rotating JavaScript challenges, backed by Android/iOS SDKs.

Allow- and deny-lists, force-identity, CAPTCHA, and rate-limiting are configurable by customer admins. Imperva deploys a forced identity challenge and a JavaScript challenge that is obfuscated and rotates every five minutes. The platform detects web-app misconfigurations, third-party JavaScript risks, and other vulnerabilities out-of-the-box or via integrated scanners.

An integrated data type classification engine scans both incoming and outgoing payloads to identify sensitive information such as PII, health records, and financial documents. Credential-stuffing and cracking attacks are mitigated through bot-driven risk scoring.

Imperva is suitable for organizations seeking a mature platform that delivers excellent WAAP capabilities. The solution is particularly well-suited for large and mid-sized organizations that require centralized policy management, advanced bot management, and DDoS protection.

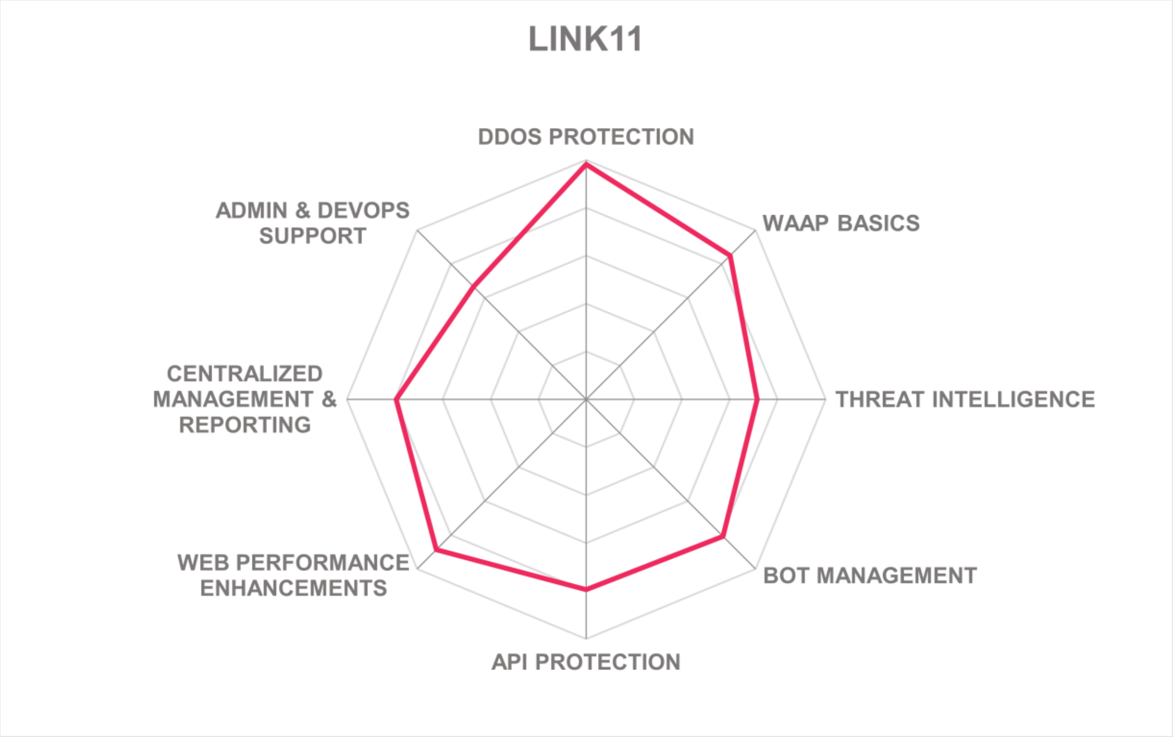
Strengths

- Has a strong market presence and partner ecosystem globally
- Strong integration capabilities with third-party solutions
- Good compliance support
- Strong utilization of ML for bot detection and ATO attacks
- A Security Operations Center (SOC) team serves as the customer escalation point for incidents, assists with investigation and remediation, and works closely with the threat intelligence team
- The admin UI presents a unified perspective of the deployed WAAP, delivering insights into web application activities via various indicators
- Strong vulnerability remediation and risk mitigation capabilities
- Effective obfuscation methods are available for sensitive data
- Dashboards and reports are both customizable and provide useful insights and metrics
- Attack Analytics report provides visibility into attack surfaces

Challenges

- Limited SDK support outside of mobile platforms
- Does not support CTI standards and has no connectors to popular CTI sources
- The API protection tool must be licensed separately, either as an add-on or a standalone solution
- No support for API routing or API key mechanisms

Link11 – Cloud WAAP



Founded in 2005 and headquartered in Frankfurt am Main, Germany, Link11 delivers a cloud-native security portfolio that includes WAAP, DDoS Protection, and CDN services. The WAAP component combines WAF, API shielding, bot mitigation, ATO prevention, and real-time traffic analytics, all managed from the unified Link11 Cloud Security Platform. Back in 2024, Link11 acquired Reblaze Technologies, a vendor that we analyzed last year in LC WAF.

Link11 Cloud WAAP operates as a SaaS platform that can be delivered through Link11 private cloud and public cloud environments. The solution also supports hybrid deployment where the control plane is deployed Link11's VPC (Virtual Private Cloud), which is also fully managed by Link11 and the data plane is hosted in the customer’s VPC. CLI tooling is limited to configuration export/import, but mobile SDKs are offered. REST API enables integration with third-party threat intelligence, virtual patching, vulnerability scanners, CDN, and SIEM solutions. However, Cloud WAAP does not currently offer integration capabilities with third-party DLP solutions. The platform maintains certifications for ISO 27001, ISO 9001, PCI DSS Level 1, and complies with BSI KRITIS, and GDPR.

Link11’s network DDoS Protection solution mitigates DDoS attacks across L3 and L4 via an Anycast scrubbing network distributed over various regions in the world. Mitigation techniques include flow-based detection, behavioral baselining, and real-time signature deployment. After the inspection by network DDoS solution, the traffic is forwarded to the Cloud WAAP for L7 inspection. Link11 maintains strong PoP coverage globally.

The automated API discovery inventories REST and GraphQL endpoints and applies OpenAPI schema validation. It also enforces rate-limit or quota rules per method or consumer. The solution provides integration with major API gateways like Kong and Apigee. While the solution supports allow-list policies, it falls short in several API protection functions, particularly the use of API key mechanisms.

Cloud WAAP's protection extends to known vulnerabilities such as the OWASP Top 10 for web and API security, as well as specific threats like SQL injection, XSS, cookie/session poisoning, and malicious payloads. The solution’s security team maintains and updates a large and growing database of web-related vulnerabilities. Cloud WAAP combines a positive security model that is built from observed application flows with proprietary negative security signatures. It also offers capabilities for custom signatures and rules, rate-limiting, geo-based rules, and flow control. These rules and signatures can be defined in either positive or negative security model depending on the user's preference. Flow Control enforces valid request sequences across user sessions and adds a behavioral security layer that helps prevent threats like session hijacking, credential stuffing, and business logic abuse.

Link11 gathers threat intelligence from its DDoS telemetry and external feeds. While their ML use cases focus on anomaly detection and false-positive reduction, the current application of ML and DL in threat hunting remains limited. The solution does not support CTI standards.

Link11 includes bot mitigation in its WAAP platform out-of-the-box. The solution employs device fingerprinting, behavioral analysis, JavaScript challenges, re-usable non-interactive puzzles, and rate-limit penalties. Passive biometrics and supervised ML classifiers are also part of the bot detection engine. The platform supports both allow-listing and deny-listing at user-agent or IP level. When it comes to vulnerability management and risk mitigation, Link11's capabilities are somewhat limited. Despite this, the solution is equipped to protect against ATO attacks and can detect credential cracking and stuffing attacks.

Link11’s Cloud WAAP is ideal for organizations seeking a managed European-operated service with integrated DDoS protection, WAAP, and CDN. It is also suitable for organizations looking for a WAAP engine that provides protection against a variety of vulnerabilities and attack vectors. However, organizations looking for advanced threat intelligence with ML capabilities or critical API protection should consider other solutions.

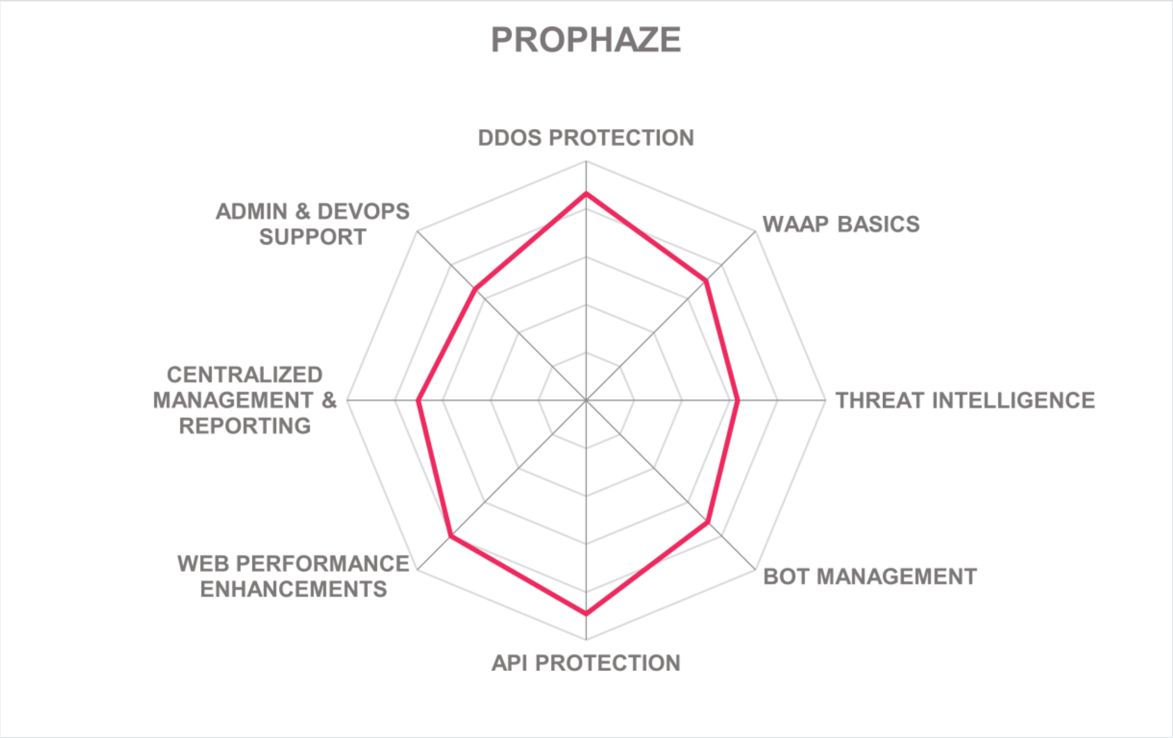
Strengths

- Mobile SDKs are supported in various programming languages. The solution is a good choice for organizations with significant mobile traffic.
- Helps organizations comply with BSI KRITIS
- Sensitive data obfuscation is supported
- User-friendly interface
- Flow Control adds a behavioral layer of defense by enforcing valid request sequences to block session hijacking and logic abuse

Challenges

- Some integration capabilities with third-party solutions are missing
- Alert prioritization is not available
- Dashboards are not customizable
- Does not support CTI standards
- Limited use of ML for threat intelligence

Prophaze – Application Security Platform



The Prophaze Application Security Platform is an all-in-one WAAP. It provides a cloud-native suite that includes traditional WAF functions, Kubernetes-native WAF, hybrid/cloud WAF, and a fully integrated API-security module. Its main features also include bot management, DDoS protection, health scoring, and CDN.

Prophaze WAAP can be deployed on-premises or in the cloud. Delivery options include SaaS, virtual appliance, container-based, software deployed to a server, or as a fully and/or partially managed service. When provided as a managed service, the solution includes all essential WAAP capabilities. Prophaze WAAP is compatible with most of the widely used container platforms. Zero-touch onboarding and AI-driven policy tuning have been recently introduced to reduce manual configuration time. The solution is built on a microservice-based architecture and can run as a Kubernetes ingress controller. IaaS installation and Prophaze-hosted SaaS remain available across major clouds. Prophaze WAAP makes most functionality available via APIs and supports SOAP, REST, TCP Socket API, and Webhooks protocols. CLI functions and SDKs are not supported. The platform integrates with threat-intelligence, SIEM, CDN, DLP, and vulnerability-scanner tools, and integrate with MISP for CTI exchange. Compliance mappings are available for GDPR and HIPAA regulations, and the PCI-DSS standard. Prophaze is a SOC 2 Type 2 certified vendor.

Prophaze WAF provides protection against various DDoS attack vectors, including L3, L4, and L7. It includes proprietary AI/behavioral detection mechanisms developed for L7 floods. The platform's architecture features moderate bandwidth thresholds and extensive global PoP coverage. It is capable of facilitating a wide range of mitigation techniques at both the application and network layers. In order to prevent DDoS attacks, Prophaze uses multiple methods including rate limiting, bot detection, IP reputation checking, behavioral analysis, and protocol validation.

The API protection solution is integrated into the WAAP solution out-of-the-box. Integration with the Kong API gateway, APG, and Azure API gateway is also possible for microservices and distributed architectures. The solution detects and discovers APIs, validates OpenAPI, REST, and GraphQL schemas, implements granular rate limiting, sensitive field masking, and risk scoring. It also allows the creation of allow lists, API routing, and the use of API key enforcement.

Prophaze WAAP provides protection against known vulnerabilities such as OWASP Top 10. The solution is capable of SSL/TLS termination and re-encryption. Both negative and positive security models are supported, with the positive security model utilizing a self-learning rule engine that auto-generates positive security rules. However, Prophaze WAAP does not currently support the use of third-party attack signatures and rules. The solution has its own out-of-the-box threat intelligence functions. CTI involves using analytics with deep inspection, ML, and DL algorithms to detect anomalies. Prophaze utilizes a combination of its own threat intelligence and intelligence from third party sources such as Anomali, Splunk, and VirusTotal, and it supports Trusted Automated eXchange of Indicator Information (TAXII) protocol for CTI sharing.

Prophaze Advanced Bot Protection is an ML-driven platform that provides bot detection and defense across AWS, Azure, and Google Cloud Platform (GCP). It utilizes PhantomJS and mouse hotspot tracking to detect vulnerabilities and proactively mitigate threats from malicious bots. The solution blocks content scraping attempts by analyzing traffic patterns and behaviors and has the ability to identify and disable scraping bots and crawlers. The solution uses activity signatures and ML algorithms to identify bot activities. The platform supports configurable allow-listing and deny-listing. Two methods are used to verify if a user is a bot: the CAPTCHA challenge and a CAPTCHA-less method that validates the browser/user agent through JavaScript.

Prophaze WAAP is equipped to with real-time alerts for excessive data exposure and third-party JavaScript risks, though native vulnerability scanning is not available. Nonetheless, it can integrate with third-party scanners such as Qualys and Tenable. The solution recognizes sensitive data and masks it in the logs.

Prophaze is a more recent entrant into the WAAP market. Despite being a newcomer in the WAAP market, Prophaze has quickly established itself by meeting most market requirements and offering a well-rounded set of WAAP capabilities with particular strength in API protection and DDoS protection. Its customers are mid-sized organizations with a small but growing market presence, mainly in India and the US as well as in other parts of the world.

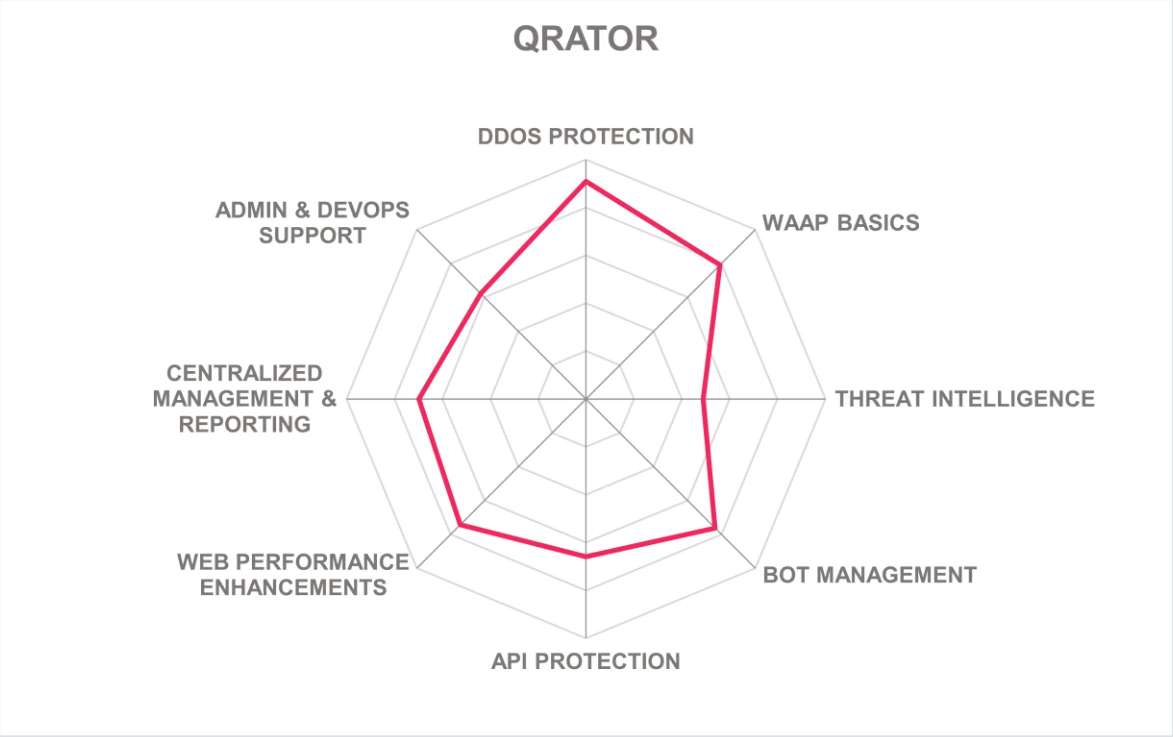
Strengths

- Support for major API protocols
- Good support for compliance and standards
- Zero-touch onboarding with minimal manual configuration time
- Strong utilization of ML algorithms for risk scoring, threat intelligence and bot management
- Integrates with the MISP project for threat data sharing
- IP reputation and anti-botnet capabilities detect vulnerabilities and proactively mitigate threats
- Obfuscation through data masking capabilities
- Health scoring provides a good overview of WAAP metrics
- An easy-to-use user interface (UI) with good dashboard graphics
- Reports provide insight into how the attacks occurred
- Strong vulnerability remediation & risk mitigation capabilities

Challenges

- Limited partner ecosystem
- CLI functions and SDKs are not supported
- Third-party attack signatures and rule sets are not supported
- Vulnerability scanning is only available for managed service customers
- Alert prioritization is not available
- Dashboards are not customizable

Qrator Labs – Qrator.WAF



Established in 2010 and based in Prague, Czech Republic, Qrator Labs provides a cloud-based, fully managed WAAP platform. Qrator Labs platform aims to address a range of web application threats, including DDoS mitigation, bot protection, and DNS protection. It also provides capabilities for service provider protection and includes CDN. Qrator Radar, a BGP (Border Gateway Protocol) monitoring solution, analyzes routing information to detect incidents and changes in network connectivity in real-time. In addition, Qrator Labs offers API protection and tools for vulnerability detection and remediation.

Qrator.WAF, also known as Solidwall, is designed to support both public and private clouds, as well as multi-cloud instances. The solution is available as a managed service or a SaaS offering. Deployment options also include virtual appliance and containers. The solution supports REST and JSON-RPC protocols. The solution integrates with some third-party tools, including SIEM platforms, CDNs, and DLP tools. No CLI or SDK interface is provided.

The solution is structured to counter a broad range of DDoS attacks across L3, L4, and L7. The solution's architecture includes moderate bandwidth limits and a significant level of PoP coverage across various regions. The solution uses a global BGP-Anycast network and scrubbing centers to filter attack traffic.

In terms of API protection, the solution provides basic API discovery capabilities and protection against malicious bots. However, it does not offer integration with an API gateway and lacks critical features such as API schema validation, API routing, and use of API key mechanisms.

Qrator.WAF uses a combination of positive and negative security rules. It incorporates ML models to build application behavior profiles, suppress false positives, and protect against OWASP Top 10 and automated threats. Qrator.SecureDNS provides distributed DNS infrastructure that resists DNS-layer attacks. The global CDN structure improves delivery performance and spreads traffic to filtering centers. Qrator.Radar processes routing data from over 800 BGP sessions with Internet Service Providers (ISPs) and CDNs. It uses proprietary algorithms to identify anomalies like route leaks, hijacks, bogons, routing loops, and DDoS amplification attempts. Alerts can be sent through syslog, email, or API.

Qrator Labs provides basic threat intelligence capabilities and tools that use unsupervised ML models to detect malicious traffic and identify false positives. They have an internal team that releases CTI reports on a quarterly and yearly basis.

Qrator.Antibot provides bot protection for websites, APIs, and mobile applications. The solution employs activity signatures such as fingerprinting and user behavior analysis, as well as ML algorithms such as clustering and weighted scoring to identify bot activity. Qrator.Antibot facilitates both allow-listing and deny-listing options to control over bot traffic. To challenge potential bots, it implements mechanisms such as background JavaScript and proof-of-work CAPTCHA. While Qrator.Antibot detects credential cracking and stuffing attacks, it has limited vulnerability remediation and risk mitigation capabilities.

Organizations that need a WAAP with a positive security model, customizable rules, and third-party signature integration should consider Qrator Labs. It is also suitable for those who need good DDoS protection and bot management capabilities. Qrator Labs has a strong market presence and partner ecosystem in Eastern Europe, making it an ideal vendor for organizations in this region. However, organizations looking for advanced threat intelligence and API protection may find Qrator Labs' offerings limited.

Strengths

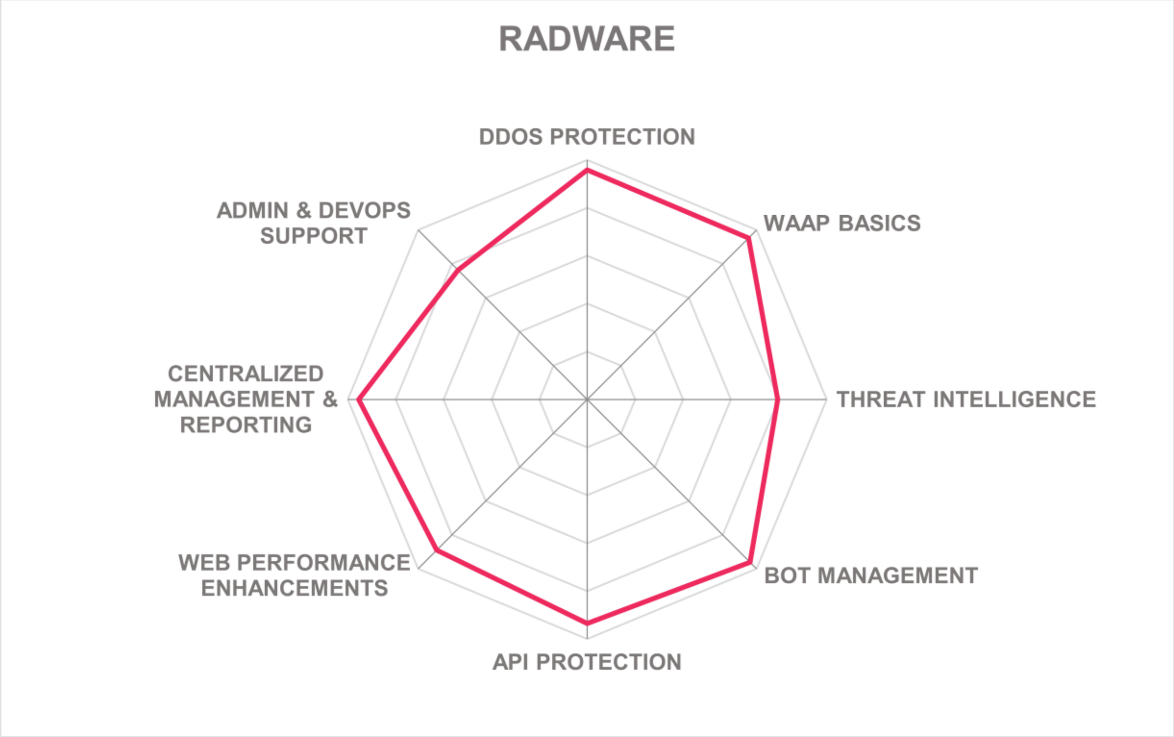
- Strong market presence in Eastern Europe
- Effective use of ML for enhancing bot management
- Easy to use and customizable dashboards
- Reports for each DDoS incident, along with monthly DDoS and bot reports, are accessible in various formats
- Two interface options, Simple and Expert, for different user groups
- Intuitive graphical policy map that clearly visualizes connections and policy relationships
- Third-party signatures and custom rules are supported
- ABAC is supported for delegated administration

Challenges

- Missing essential integrations with third-party solutions
- Lack of compliance and standards support

- More automation is needed to improve the user experience when using the platform.
- Critical API security features such as API schema validation, API routing, and API key mechanisms are not supported.
- Passive biometrics are not used for bot detection
- Limited vulnerability remediation & risk mitigation capabilities
- Limited threat intelligence capabilities
- No support for DevSecOps tools
- No support for CLI or SDK

Radware – Radware Suite



Leader in

OVERALL LEADER
PRODUCT LEADER
INNOVATION LEADER
MARKET LEADER

Established in 1996, with its headquarters in Tel Aviv, Israel, Radware delivers a unified WAAP portfolio that includes Alteon with integrated WAF, Cloud WAAP Service, Kubernetes WAF, Bot Manager, Cloud DDoS Protection Service, and DefensePro. The Radware Suite also provide tools for web and mobile application protection, API discovery, threat intelligence, CDN, client-side protection, and AI SOC Xpert, a set of ML and gen-AI engines used across Radware products for real-time detection, policy tuning, and cross-signal correlation.

The Radware Suite supports several deployment models, including on-premises appliances, virtual appliances, public-cloud instances, and Radware-hosted SaaS. Kubernetes WAF micro-services offer container-native protection, and coverage extends to Docker, Rancher, Red Hat OpenShift, and other orchestration platforms. A managed WAAP delivery option allows it to be partially or fully managed by Radware, its partner, or the customer. Kubernetes WAF can be fully managed via CLI. Radware Suite also provide support for SDKs. It offers integration with a few third-party virtual patching, CDN, SIEM, vulnerability scanners, and API gateways, yet it lacks several critical out-of-the-box connectors with complementary solutions to WAAP. REST APIs are provided for third-party integrations. Radware's products and services have been independently certified to support a wide range of regulations and standards, such as PCI-DSS, NIS2, and Securities and Exchange Commission (SEC). Furthermore, Radware has achieved ISO 27701 and SOC 2 Type 2 certification, and aligns with GDPR and DORA regulations.

DefensePro and Cloud DDoS Protection protect against L3, L4, and L7 DDoS and DoS attacks, as well as providing low latency, high bandwidth capacity, and a good forwarding rate. The architecture of the solution provides excellent coverage of PoPs and scrubbing centers worldwide. Radware deploys behavioral-based detection and automatically generates real-time signatures to block zero-day network and application attacks including HTTPS flood attacks

The Radware Suite uses an automated API discovery algorithm and creates custom policies to identify and block attacks targeting the API attack surface. Compatible with multiple API gateways, the Radware Suite performs schema validation for documented APIs using OpenAPI. For undocumented APIs, its discovery feature automatically constructs OpenAPI artifacts. In addition, the solution provides API quota management for implementing rate-limiting functionality. While allow lists, BOLA detection, and API rate limits are available, API routing is not natively provided. API key exchange mechanisms for authentication and authorization are supported by Radware.

The solution provides protection against known vulnerabilities such as OWASP Top 10 for web, OWASP Top 10 for API Security, OWASP Top 10 Client-Side Security Risks, and OWASP Top 21 Automated Threats. It uses a hybrid security model that combines a positive engine, which learns application behavior, and a negative engine, which is driven by proprietary signatures. However, the solution does not use third-party signatures and rules.

The Radware Suite leverages both internal and external sources for threat intelligence and has strong capabilities in this area. Radware CTI combines Radware’s global deception network with external feeds and is distributed as the Emergency Response Team (ERT) Active Attackers Feed.

Radware Bot Manager features a unique semi-supervised ML algorithm that identifies the intent of each request. It employs intent-based deep behavioral analysis, passive biometrics, and AI-based device fingerprinting to classify traffic. High-risk bots receive tough challenges, including the Crypto Challenge, which aims to exhaust automated tools that use AI-driven CAPTCHA solving. IDBA (Intent-based Deep Behavioral Analysis) uses the latest developments in DL to give zero-day protection to applications and reduce false positives. Radware includes basic bot defense mechanisms in its base tier, while more sophisticated bot protection features are available in the complete tier for an additional fee. The Bot Manager provides a range of allowlisting and customizable denylisting options as well.

While Radware's vulnerability remediation and risk mitigation capabilities are somewhat limited, integration with external vulnerability scanners is supported. Radware's WAAP engine incorporates DLP through data masking filters that hide sensitive data and remove it from logs. Client-side protection maps and monitors third-party scripts to detect skimming, formjacking, and other browser-side risks.

Radware offers strong support across the board for organizations ranging from small to medium and large enterprises. Their customer base is equally represented in North America, EMEA, and APAC regions, with expansions into Latin America and a strong partner ecosystem in the respective areas. Radware is highly innovative and should be considered when evaluating an organization's WAAP.

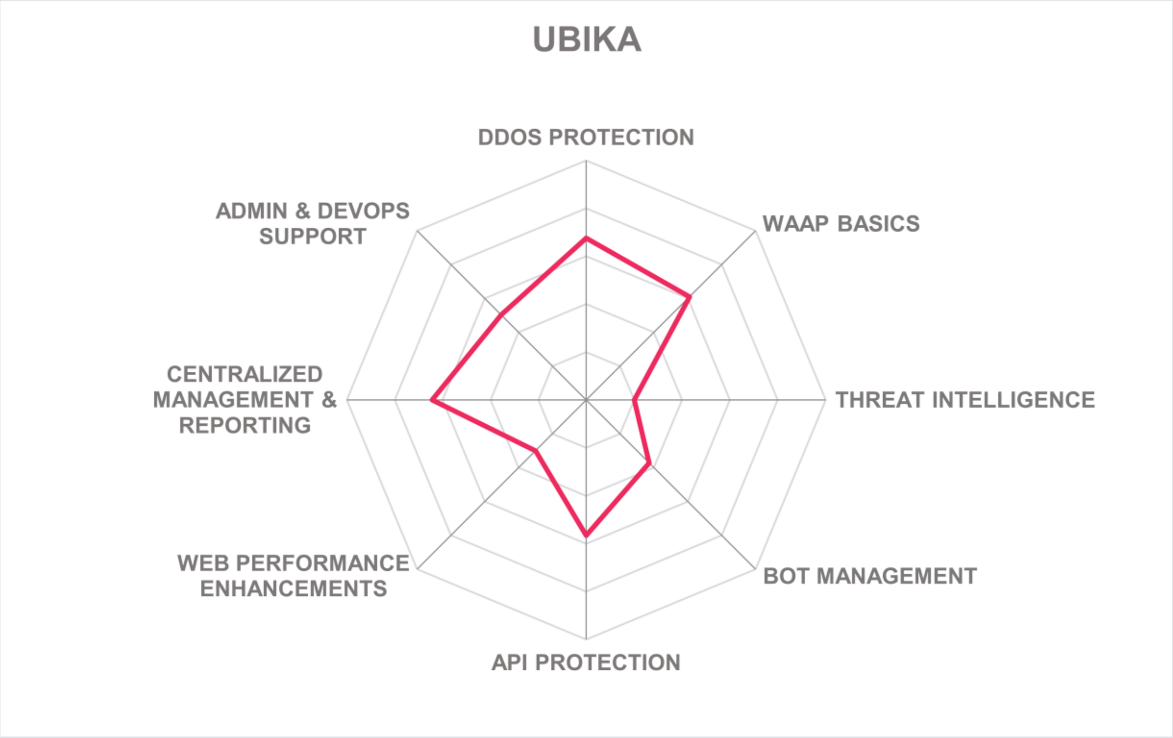
Strengths

- Strong partner ecosystem and global market presence
- Extensive support for various compliance requirements
- API attack surface protection
- Effective use of ML and DL to protect against malicious bots and zero-day attacks, and to minimize the number of false positives
- Innovative CAPTCHA-less crypto challenges that leverage blockchain-inspired cryptographic mechanisms
- Automated security policy generation and automated continuous policy optimization
- All Radware's solutions come with a reporting and actionable analytics engine
- A member of the CTA (Cyber Threat Alliance) and it supports various CTI standards
- Obfuscation through data masking filters
- The emergency response team provides in-depth threat research and support to mitigate security incidents
- AI SOC Xpert engine enhances the platform's ease of use
- Bot protection for mobile apps and platforms
- Strong client-side protection that secures the digital supply chain

Challenges

- Some critical out-of-the-box integrations are missing
- Third-party attack signatures and rule sets are not supported
- Limited vulnerability remediation and risk mitigation capabilities
- Advanced bot protection features are not available in the standard plan

UBIKA – UBIKA WAAP Gateway



Established in 2001 and headquartered in Meudon, France, UBIKA offers a broad portfolio of security solutions and is a member of Total Specific Solutions (TSS), a global provider of IT business solutions. UBIKA WAAP protects web applications and APIs from various threats and exploits. It provides protection against SQL injection, XSS, zero-day exploits, distributed DDoS attacks, and malicious bots. In addition, the solution features virtual patching and DLP-like filtering and supports CDN acceleration. UBIKA offers four distinct products for different deployment and delivery options: UBIKA WAAP Gateway for on-premises, UBIKA WAAP Gateway for cloud, UBIKA Cloud Protector, and UBIKA WAAP Container.

UBIKA WAAP Cloud is based on a reverse-proxy architecture and can be deployed via the UBIKA WAAP Gateway. It is available for on-premises hardware and virtual appliances, and as SaaS. The Cloud Edition supports IaaS environments like AWS, Azure, and GCP, and container-native edition supports Docker, Kubernetes, OpenShift, and Rancher Labs. UBIKA has mostly microservice based architecture, except for some legacy components. SDKs are not available, but CLI functions are provided in the SaaS product for management tasks. The full range of UBIKA WAAP Gateway's features can be accessed through its API, with support for API protocols including REST, XML-RPC, gRPC, and GraphQL. The solution does not integrate with some essential third-party tools, but it does integrate with threat intelligence solutions such as Webroot and SIEM solutions like Splunk. UBIKA supports compliance with CSPN (Certification de Sécurité de Premier Niveau) and ANSSI, France based regulations.

UBIKA WAAP offers protection against L3, L4, and L7 DDoS attacks. The level of protection against DDoS attacks varies depending on the four UBIKA products. It provides a moderate level of bandwidth capacity and has PoPs in most regions. DDoS protection and WebSocket acceleration utilize UBIKA's EU-hosted Anycast network.

The UBIKA Gateway and UBIKA Cloud Protector provide essential tools for API discovery and protection, including OpenAPI and JSON schema validation, API routing, API authentication, rate-limiting, and the capability to build an allow list. This list can be auto-generated using intelligent techniques or rule-driven methods. The API security features include support for the OWASP Top 10 API Security risks, as well.

The UBIKA WAAP products provide protection against OWASP Top 10 web application vulnerabilities. The solutions also provide both negative and positive security models. The negative model allows for signature-based and rule-based approaches, while the positive model can be automatically configured with automatic learning or Swagger/OpenAPI 3 upload. Security policies are specified visually and via graphical workflow rules that are supporting rate-limiting, geofencing, and signatures. However, third-party attack signatures and content validation policies are not supported.

The threat intelligence is limited to integration with Webroot. UBIKA workflows can also connect to external APIs to get more threat information about the clients.

Bot mitigation is present in the WAAP out-of-the-box. The solution has somewhat limited bot management capabilities and cannot utilize activity signatures, passive biometrics, or ML to detect bots. It can provide a challenge-based approach to allow-list legitimate web clients while blocking malicious bots. However, UBIKA has recently updated their bot mitigation engine, and they are working on improving detection accuracy and performance by supporting automatic rule generation. A basic tool for vulnerability remediation and sensitive data protection is offered. It can detect and obfuscate PII in API traffic using encryption techniques to protect sensitive data in transit.

UBIKA focuses on mid-market to enterprise organizations and supports companies in regulated industries, such as healthcare, primarily in the EMEA region, and with some presence in the APAC region and North America. It is used by sectors such as government, finance, and insurance to protect sensitive file transfers, webmail access, and API channels for collaboration tools from external threats. UBIKA WAAP solutions provide WAAP features with decent DDoS and API protection capabilities.

Strengths

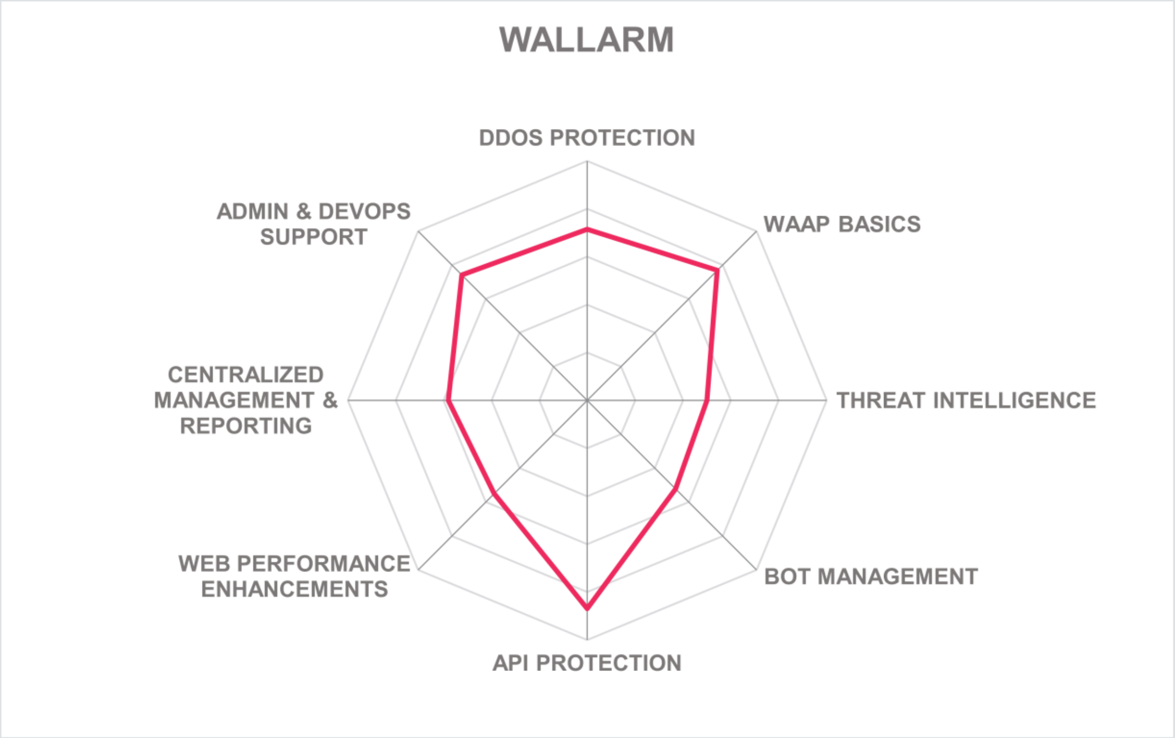
- Strong partner ecosystem within the EMEA region
- Smart graphical UI
- A WAAP solution built on a true gateway architecture
- Support for major API protocols

- Policies can be defined visually or via workflows
- One of the few vendors that actively protects WebSocket traffic, not just monitors it
- Strong focus on healthcare sector

Challenges

- Missing reports for major compliance frameworks out-of-the-box
- Bot detection methods are limited
- Passive biometrics are not used for bot detection
- Integration with critical third-party solutions, such as vulnerability scanners and API gateways, is missing
- Limited use of AI and ML algorithms for threat and bot detection
- SDK support is missing
- Threat intelligence capabilities are only available through third-party solutions
- Third-party attack signatures and content validation policies are not supported.

Wallarm – Cloud-Native WAAP



Wallarm, established in 2016 and headquartered in San Francisco, California, provides an application and API security platform composed of three modules: Cloud-Native WAAP for real-time web and API protection, Advanced API Security for abuse prevention and credential stuffing detection, and API attack surface management for inventory and leak monitoring. The Cloud-native WAAP also provide tools for virtual patching, geo-based blocking, distributed rate limiting, behavior-based attack mitigation, and protection against ATO attacks and zero-day vulnerabilities. Even though the unified platform lacks functions like fraud detection and CDN, it includes all essential WAAP capabilities such as DDoS protection, bot management, vulnerability detection and remediation, and threat intelligence.

As a cloud-native solution, Wallarm's platform is deployable across various instances, including multi-cloud and hybrid environments. Lightweight filtering nodes deploy as Docker containers, Kubernetes ingress controllers, or on load balancers across public cloud, hybrid, or on-premises environments, while policy management and analytics reside in Wallarm Cloud. The platform is available as SaaS, integrates with API gateways, and is also offered as a partially managed service. While not a fully managed service, customers receive proactive monitoring of their systems, false positive identification, and a dedicated Slack channel for support. All capabilities are exposed through REST APIs and Webhooks for integration with SIEM, DevOps, ITSM, virtual patching, vulnerability scanner, and log-management platforms. Out-of-the-box integrations are provided with third-party platforms like Qradar, Elasticsearch, Slack, and Jira. The platform lacks CLI support and does not offer SDKs for developers. Wallarm provides connectors to third-party API protection platforms and enables the ingestion of traffic from various solutions, including Cloudflare, Akamai, API gateways, and CDNs. However, the platform does not integrate with threat intelligence solutions. Wallarm holds SOC 2 Type 2 and SecureIQLab, a cloud validation provider, certifications.

Wallarm’s platform provides partial protection against L7 DoS and DDoS attacks such as data bombs, brute force attempts, forced browsing, supported with good bandwidth limits, and globally distributed PoP coverage. Wallarm needs to expand its coverage of DDoS attack types. While proficient in most L7 mitigation methods, L3 and L4 DDoS protection is delivered via a separate DDoS service.

Within its WAAP subscription, Wallarm supports REST API, SOAP, GraphQL, gRPC, and Webhooks and offers advanced API security capabilities. Some of these API protection capabilities are available separately as part of the Advanced API Security solution. Additionally, API leak detection is available as part of the API Attack Surface Management solution. API Attack Surface Management is where Wallarm enables visibility into exposed APIs and their associated risks across environments. Wallarm assigns a risk score to each detected API based on its attributes such as authentication status, exposure, and sensitivity. The system identifies and classifies Rogue, Shadow, Orphan, and Zombie APIs. API Protection provides endpoint discovery and enforces traffic based on API definitions. The API Firewall performs real-time validation of requests and responses using OpenAPI and GraphQL schema validation. The platform also supports shadow-API discovery in monitoring mode and applies rate limiting and quota controls per endpoint. Behavioral analysis and ML-based engines detect API abuse such as unusual query patterns, suspicious user agents, and credential stuffing. IP and geo-location filtering enables denylists and greylists to prevent access from specific data centers, service providers, and regions/countries. The interface shows detailed logs of API activity across different protocols like GraphQL, SOAP, and gRPC. It displays the actual queries and interactions that occur, so users can see what data is being requested or sent, how APIs are being used, and spot any unusual or risky behavior.

Wallarm’s platform presents an overview of system protection against known vulnerabilities such as the OWASP API Top 10 and zero-day exploits. It provides configuration options to deploy both positive and negative security models. With the negative model, the solution uses token-based, rule-based, and ML-based detection methods. On the other hand, the positive model allows customers to enforce API specifications on a case-by-case basis. Positive security enforcement can be enabled per API by uploading specifications, while negative security rules leverage Wallarm’s proprietary detection engine and custom regular-expression imports.

The solution integrates threat intelligence to identify malicious traffic and uses ML algorithms to support WAAP detection capabilities. In addition, Wallarm leverages its proprietary threat intelligence and malicious IP feeds for blocking and policy customization. However, it lacks support for CTI standards and protocols.

Wallarm's bot management employs ML and behavioral analysis to separate human and automated traffic without passive biometrics. The solution differentiates between malicious API bot activity and legitimate bots using ML-based detectors. This allows clients to allow-list or deny-list specific bots and configure policies separately. Wallarm delivers API bot management capabilities driven by ML and addresses a functionality that is still uncommon in the current market. Wallarm does not include challenge methods to detect potential bot activities. However, it offers visual analysis tools to investigate blocked bots.

In terms of vulnerability mitigation, the platform provides basic vulnerability assessment and active threat verification tools as part of its standard plan. More advanced features, such as API leak detection, risk scoring, and security testing require additional licensing. Wallarm's Cloud WAAP automatically applies virtual patches to identified vulnerabilities. In addition, the solution effectively detects sensitive data, such as personal and financial information and removes it from logs. To prevent stolen credentials, the platform employs various protection measures, including brute-force triggers, behavioral analysis, rate limiting, and credential stuffing detection.

The Wallarm platform is a strong fit for organizations that prioritize API discovery and protection within a WAAP solution. However, it may not meet the needs of those seeking L3 and L4 DDoS mitigation or advanced bot management capabilities. The platform offers two distinct plans: basic and advanced and extends protection across diverse environments.

Strengths

- Effective use of ML algorithms for threat intelligence
- Advanced API protection with discovery, schema validation, and abuse detection
- Good vulnerability remediation and risk mitigation capabilities
- Data masking functions provide capabilities for sensitive data protection
- Integrates with various third-party API gateways
- Visual API activity logs and interaction tracing across protocols
- Filtering nodes can be deployed in third-party CDN solutions
- Strong credential protection and brute-force defenses
- The dashboard presents a variety of statistics and metrics, such as the API protocols used, API discovery and leaks, authentication techniques, and detected sensitive data

Challenges

- Compliance support needs to be expanded
- L3 and L4 DDoS protection requires separate service
- No support for CLI or SDK
- Limited bot management capabilities
- Passive biometrics are not supported for bot detection
- Does not understand CTI standards and protocols
- Some advanced API protection features require additional licensing

Vendors to Watch

Besides the vendors covered in detail in this document, we observe some other companies in the market that readers should be aware of. These vendors did not participate in the rating for various reasons but nevertheless offer a significant contribution to the market space.

Akamai – App & API Protector

Akamai Technologies is headquartered in Cambridge, Massachusetts, USA. Founded in 1998, the company is one of the veteran players in the market, providing a broad range of security, performance, and edge services. Akamai's App and API Performance offering utilizes its CDN to enhance application and API performance and availability and intelligent load balancing. Its App & API Protector offering provides the capabilities expected from a modern WAAP. In addition to protection against the OWASP Top 10, it also offers DDoS protection, bot mitigation, API discovery and protection, automated updates, and self-tuning.

Why worth watching: Akamai's App & API Protector is a WAAP solution that integrates web application firewall, bot mitigation, API security, and L7 DDoS protection into a single platform. Its WAF approach helps organizations adapt to the evolving threat landscape with automated and proactive actions.

Barracuda Networks – Barracuda WAF

Barracuda Networks, founded in 2003, is an IT provider of security and storage solutions headquartered in Campbell, California, with offices worldwide. Barracuda Networks Cloud Application Protection provides WAAP protection for workloads in the cloud. The product offer WAF capabilities, DDoS protection, bot management, API security, and automated security policy compliance. Threat intelligence is based on its global network of sensors and customer traffic, providing ML-based and near real-time detection of threats. The Barracuda WAAP can be delivered as a hardware or virtual appliance deployed on-premises or as a container hosted in the cloud.

Why worth watching: Barracuda Networks continues as a provider of WAF-as-a-Service, providing essential WAAP.

Cloudflare – WAF, Bot Management, API Protection, DDoS Protection

Founded in 2010, with headquarters in San Francisco, California, Cloudflare focuses on web infrastructure, zero trust, and application security solutions. The company has quickly grown from providing a simple “firewall in the cloud” to one of the leading website performance and security services providers. Cloudflare provides a baseline set of WAF capabilities, bot management, API protection, and advanced WAF intelligence. It also offers tools for ATO protection, fraud detection, virtual patching, CDN, and DLP. Cloudflare's managed rules protect against known vulnerabilities and zero-day threats. ML is utilized to detect attack vectors such as SQL injections, XSS, and RCE (Remote Code Execution). They provide both free and enterprise plans for WAF, bot management, and DDoS protection.

Why worth watching: Cloudflare offers a strong edge network of its own, although it provides no other deployment alternatives to its customers. Cloudflare provides a good set of WAF, bot management, and API protection capabilities, which should interest organizations considering its web protection options.

Ergon – Airlock Secure Access Hub

Ergon is a Swiss-based company established in 1984 with over 20 years of experience in application security and access management. Airlock is a single security product by Ergon with multiple services within the Secure Access Hub. The components of Secure Access Hub include Airlock Gateway, Microgateway, and IAM products, which can be separately licensed. Airlock Gateway serves as a WAAP solution and provides users with a WAF engine and API security gateway. Airlock includes additional functions such as web traffic filtering, Layer 7 DoS protection, bot management, API protection, and virtual patching. It also provides protection against credential stuffing, password spraying, and account enumeration. With Airlock Microgateway, an alternative deployment option for Kubernetes is available.

Why worth watching: Airlock has a well-established and mature set of IAM and WAAP products with a strong focus on basic WAF, bot management, and API protection capabilities. Ergon Airlock Secure Access Hub continues to grow its feature set and remains an interesting alternative to other solutions within the DACH EMEA region.

Fortinet – FortiWeb & FortiWeb Cloud

Founded in 2000 and based in Sunnyvale, California, Fortinet is a cybersecurity company known for its extensive range of security gateways and tools. Within this portfolio, FortiWeb platform specifically addresses web applications and API security. The platform includes ML driven threat detection that is designed to protect applications from vulnerabilities and zero-day threats. FortiWeb also provides bot mitigation, API detection and protection, and mobile application protection. Threat analytics capabilities help FortiWeb users simplify attack investigations. FortiWeb provides protection against DDoS attacks, stolen credentials, and delivers API protection that extends to mobile environments. Equipped with tools for threat intelligence, vulnerability detection and remediation, virtual patching, DLP, and CDN, FortiWeb is a strong player in WAAP market.

Why worth watching: FortiWeb is suitable for enterprises seeking WAAP with advanced bot management, and threat intelligence capabilities that provide sophisticated security strategies for organizations.

Fortra – Fortra Managed WAF

Founded in 1982 and headquartered in Eden Prairie, Minnesota, Fortra provides a range of cybersecurity solutions and managed services. Their offerings cover various facets of cybersecurity, including vulnerability management, digital risk protection, email security, threat intelligence, penetration testing, and managed services such as detection and response, WAF, data loss prevention, and integrity management.

Why worth watching: Fortra WAF is a managed security solution that includes essential WAAP capabilities. In 2023, Fortra made progress in offensive security with notable acquisitions such as Outflank, a Dutch organization.

HUMAN Security – Human Defense Platform

HUMAN is a cybersecurity company based in New York, New York, United States. The company started as White Ops, then later acquired by Goldman Sachs in 2020. White Ops has since reintroduced itself as HUMAN. HUMAN Defense Platform protects websites and mobile apps from bot attacks. HUMAN's detection engine gives actionable insights regarding digital transactions across networks and devices to protect against fraud and secure user accounts. Intelligence is collected from applications, APIs, IoT (Internet of Things) devices, and advertising platforms to identify anomalies in internet traffic patterns through AI/ML. The solutions policy engine allows customers to define rules and policies that determine what traffic gets through.

Why worth watching: HUMAN Security provides advanced bot management and solid protection for client-side threats.

MYRA Security – Application Security

Myra Security, founded in 2012 and headquartered in Munich, Germany, delivers WAAP via its Myra Security Application Security platform. The solution unifies WAF, DDoS protection, bot mitigation, and CDN capabilities to defend against a range of threats. Myra operates under German data sovereignty frameworks aligned with GDPR and BSI-certified infrastructure. It supports regulated sectors, including finance, healthcare, e-commerce, government, and organizations with critical infrastructure.

Why worth watching: Myra Security suits for organizations in Germany and the wider DACH region. It is a good alternative for organizations seeking a fully managed cloud WAAP backed by 24/7 SOC support.

Oracle – OCI Web Application Firewall

Based in Texas, Oracle has been a leading provider of cloud infrastructure, database management, and enterprise resource planning software since 2016. The Oracle Cloud Infrastructure (OCI) WAF is based on Zenedge technology, which was acquired by Oracle in 2018. OCI WAF is offered to its customers as a cloud-based managed service.

Why worth watching: The OCI WAF provides good core WAF capabilities with strength in the number of signature rules to choose from. The Oracle WAF may be of interest to existing OCI customers.

Palo Alto Networks – Cortex Cloud WAAS

Palo Alto Networks, founded in 2005 in Santa Clara, CA, is a multi-national cybersecurity company, a leading provider of traditional network security tools and modern cloud-native security solutions, and a pioneer in Next-Generation Firewall (NGFW) technology. The Web Application and API Security (WAAS) is the Palo Alto Networks platform for securing infrastructure, applications, and data, focusing on cloud-native applications across VMs, container and Kubernetes applications, PaaS platforms, and serverless applications.

Why worth watching: Palo Alto Networks' WAAS is a cloud-native platform that provides integrated security throughout the application lifecycle and across cloud architectures. It is built on a modern architecture with a good set of deployment and delivery options. The solution offers advanced protection for web applications and APIs, leveraging ML and threat intelligence to defend against sophisticated attacks.

Peakhour – Peakhour WAAP

Peakhour, founded in Australia and headquartered in Sydney, delivers its WAAP solution through a DNS-based cloud-native architecture. The platform integrates key capabilities such as WAF, bot protection, advanced rate limiting, API protection, DDoS mitigation, Transport Layer Security (TLS) management, and fraud prevention. It also provides performance-oriented features including full-page caching, image optimization, origin shield, and content acceleration.

Why worth watching: Peakhour is one of the few WAAP vendors based in Australia. Its service model and infrastructure are well-suited for the Australian and broader Asia-Pacific markets. The modular design of its platform allows organizations to choose only the components they need. This makes Peakhour a cost-effective and flexible option. It serves as a solid choice for SMBs looking for a simplified, yet capable WAAP solution tailored to their needs.

Sense Defence – Next-Gen Cloud WAF

Sense Defence is a London-based company established in 2022 that offers an AI-powered WAF solution. Their enterprise plan includes DDoS prevention, bot management, rate limiting, threat intelligence, virtual patching, and managed SSL/TLS certificates. The solution utilizes dynamic profiling and behavioral analysis to implement mitigations. The platform provides protection against known web application vulnerabilities and some custom APIs against sophisticated attacks.

Why worth watching: With its scalable adaptability and user-friendly interface, this solution is suitable for small to medium organizations looking for managed services and customized solutions.

ThreatX – ThreatX Cloud WAF

Founded in 2014 and located in Louisville, Colorado, United States, ThreatX is a company focused on web application and API protection through its WAAP solution. ThreatX takes a behavior-based and intelligence-centric approach to WAFs. Its risk engine provides traditional WAF and API protection, bot mitigation, and DDoS protection as examples. ThreatX provides more advanced WAF features out-of-the-box using their behavioral analytics approach to threat detection, such as multiple sources of threat intelligence to help mitigate web attacks, as well as more traditional signature rule policies. ThreatX offers agentless container-based reverse proxy deployment options that support both cloud and on-premises deployment models. In addition, a managed service is also available.

Why worth watching: ThreatX provides innovative strategies for protecting web applications and APIs.

United Security Providers – USP Secure Entry Server

Providing IT Security for more than 25 years, United Security Providers (USP) is a Swiss software vendor and service provider owned by Swisscom with offices in Bern (headquarters), Zurich, and Minsk. USP has more than 100 security professionals and operates its own 24/7 Security Operations Center. The USP Secure Entry Server® (SES) offers a modular suite that includes Web Access Management, Identity Federation, Single Sign-on, and Web Application Firewall capabilities.

Why worth watching: United Security Providers Secure Entry Server's offering provides good core WAAP capabilities that will interest potential customers in their primary target DACH region.

Related Research

Leadership Compass - Fraud Reduction Intelligence Platforms - Finance

Leadership Compass - Cloud Native Application Protection Platforms (CNAPP)

Leadership Compass - Attack Surface Management (ASM)

Leadership Compass - Enterprise Secrets Management

Leadership Compass - Access Management

Leadership Compass - Cloud Security Posture Management

Leadership Compass - Security Orchestration, Automation, and Response (SOAR)

Leadership Compass - Data Security Platforms

Leadership Compass - eXtended Detection and Response (XDR)

Leadership Compass - Managed Detection and Response (MDR)

Leadership Compass - Network Detection and Response (NDR)

Leadership Compass - Endpoint Protection Detection & Response (EPDR)

Leadership Compass - Intelligent SIEM Platforms

Leadership Compass – API Security and Management

Buyer’s Compass – API Security and Management

Executive View - Airlock Secure Access Hub for Applications and APIs

Advisory Note - Cyber Insurance - Coverage Types and Technical Requirements

Advisory Note - Comparison of National Cloud Security Standards

Whitepaper - NIS2 Starts with Securely Managed Endpoints

Copyright

The conclusions, recommendations, and predictions in this document reflect KuppingerCole's initial views. As we gather more information and conduct deeper analysis, the positions presented here may undergo refinements or significant changes. KuppingerCole disclaims all warranties regarding the completeness, accuracy, and adequacy of this information. Although KuppingerCole research documents may discuss legal issues related to information security and technology, we do not provide legal services or advice, and our publications should not be used as such. KuppingerCole assumes no liability for errors or inadequacies in the information contained in this document. Any expressed

KuppingerCole Analysts supports IT professionals with exceptional expertise to define IT strategies and make relevant decisions. As a leading analyst firm, KuppingerCole offers firsthand, vendor-neutral information. Our services enable you to make decisions crucial to your business with confidence and security.

Founded in 2004, KuppingerCole is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as technologies enabling Digital Transformation. We assist companies, corporate users, integrators, and software manufacturers to address both tactical and strategic challenges by making better decisions for their business success. Balancing immediate implementation with long-term viability is central to our philosophy.

For further information, please contact clients@kuppingercole.com..