aws marketplace

Radware Cloud WAF Service

Reviews, tips, and advice from real users








Powered by PeerSpot

Contents

Product Recap . . . . . 3 - 4

Valuable Features . . . . . 5 - 16

Other Solutions Considered . . . . . 17 - 19

ROI . . . . . 20 - 22

Use Case . . . . . 23 - 27

Setup . . . . . 28 - 31

Customer Service and Support . . . . . 32 - 34

Other Advice . . . . . 35 - 37

Trends . . . . . 38 - 39

About PeerSpot . . . . . 40 - 41

©2026 PeerSpot, All Rights Reserved



Product Recap

Radware Cloud WAF Service

Radware Cloud WAF Service Recap

Radware Cloud Application Protection Services is a cloud-delivered service that protects web applications and APIs across all environments against any type of application layer attack. It includes an advanced WAF, bot and AI agent trust management, account takeover protection, API security, DDoS protection, LLM firewall, vulnerability management, threat intelligence, and client-side protection. It uses AI-driven behavioral analysis to distinguish legitimate from malicious traffic and automatically adapt security policies, protecting against known vectors such as the OWASP Top 10, API Top 10, Top 21 automated threats, LLM Top 10, and more, as well as business logic attacks and supply chain attacks on the client side. The service is delivered through a global network of points of presence and scrubbing centers, using a proprietary API-based architecture that also allows for deployment without DNS changes, traffic rerouting, or SSL key sharing. It supports on-premises, private cloud, public cloud, and hybrid environments, helps organizations comply with standards such as PCI DSS 4, NIS2, GDPR, HIPAA, and DORA, and includes threat intelligence and 24x7 managed security support.

Radware Cloud Application Protection Services are offered through a subscription-based pricing model, with fees determined by selected service tiers and specific application coverage required by the client. The service is structured to provide different levels of protection and features, and cost is typically based on factors such as the number of applications, bandwidth usage, and specific security functionalities included in the chosen package.

©2026 PeerSpot, All Rights Reserved

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- "The proactive and holistic approach based on correlation between modules has been effective in protecting my applications since, as the modules are from the same vendor, they allow us more native integration and they operate more efficiently."



Carla Vega

Defensive cybersecurity engineer at a financial services firm with 1,001-5,000 employees

- "Radware Cloud WAF Service has positively impacted my organization by providing peace of mind for the team and regulatory compliance, since having the application properly protected meets our banking field requirements."



Validated user

Experto de Seguridad Informática at a financial services firm with 1,001-5,000 employees

- "We are achieving six to seven ms latency, so we are very much happy with the performance and the solution uses."



Validated user

Program Manager at a insurance company with 1,001-5,000 employees

©2026 PeerSpot, All Rights Reserved

"Due to Radware Cloud WAF Service, we have provided more security to the applications and have protected our applications from attackers with the best service."



Vishal Salve

manager at a financial services firm with 201-500 employees

"The DDoS attack mitigation and bot mitigation have worked well for us, as we implement rate limits to requests and block connections from countries like China where we don't have clients, which has helped us to identify and block these attacks."



Yogesh Dayma

Assistant Director Of IT at a non-profit with 1,001-5,000 employees

"I am currently satisfied with Radware Cloud WAF Service because it is a great tool to protect Layer 7 applications."

Validated user

Assistant Manager (Network and Cyber Security) at a manufacturing company with 1,001-5,000 employees

©2026 PeerSpot, All Rights Reserved

"Radware Cloud WAF Service offers great features including Bot Manager, path access, RFC-related signatures blocking, ACL, API protection, and load balancing, with every feature having its own benefits tailored to each application."



Validated user

Network infrastructure lead at a financial services firm with 501-1,000 employees

©2026 PeerSpot, All Rights Reserved

What users had to say about valuable features:

"The best features that Radware Cloud WAF Service offers include my involvement in multiple projects; one was four years ago, and one was two years ago, where we successfully implemented Radware Cloud WAF Service for both projects.

"The features of Radware Cloud WAF Service that stood out to me the most were suggested by our cyber security division at the start of the project, and we successfully implemented those features.

"I would add that we had some security issues in one project where we found our site had been hacked, and some malicious files were injected into our server.."

Validated user

Solution designer at a government with 10,001+ employees

Read full review

©2026 PeerSpot, All Rights Reserved

“Radware Cloud WAF Service offers blocking and monitoring logs, so if I want to block any kind of traffic, I can block it, and if I want to monitor, then I can monitor. These fields are good.

“Automated application mapping is good.

“I am accessing Radware Cloud WAF Service for blocking unknown threats and attacks in terms of API DDoS, geo-blocking, data leak prevention, and bot protection.

“Bot protection is really helpful for our organization to mitigate bot traffic and identify and block that traffic so that we can prevent unnecessary attacks.

“Automated analysis in Radware Cloud WAF Service is good and really helpful for us to identify the events and the traffic in those events to clarify bot traffic or unnecessary traffic and genuine traffic so that we can take the required action accordingly.

“With our existing application APIs and SIM monitoring tools, Radware Cloud WAF Service makes it easier to centralize security visibility and correlate the WAF events with other security and application data..”

YogeshTalekar
Associate at Mirae Asset Capital Markets (I) Pvt Ltd

Read full review

©2026 PeerSpot, All Rights Reserved

"Radware Cloud WAF Service offers great features including Bot Manager, path access, RFC-related signatures blocking, ACL, API protection, and load balancing. I can implement a BCDR concept where if production in the data center fails, it automatically switches to the disaster recovery site.

"This includes application redirections, access path protections to safeguard against SQL injections, cross-site scripting protections, and blocking malicious IP addresses in my environment.

"I find that every feature has its own benefits tailored to each application, such as API protection for API applications and Bot Manager for all applications. Each feature supports the overall security needs of internet-hosted applications.

"When onboarding applications, I publish a CNAME over my DNS hosting service and initially put the application in learning mode, allowing specific vendors to access it. I tighten access rules based on this testing. After completing the learning phase, I transition to blocking mode, enabling protections against SQL injections and implementing the Bot Manager and API protections as required.

"Every day, my team reviews analytics from Radware Cloud WAF Service to observe anomalies and attack patterns. I compile this information to enhance my other security measures, ensuring comprehensive protection and data integrity across environments.

"I have an API key and use on-premises solutions with Amazon S3 for log fetching. I aim to push captured logs from Radware Cloud WAF Service to my on-premises systems using this API integration.

"Radware Cloud WAF Service has a robust set of protections against zero-day attacks. Whenever new vulnerabilities arise, I receive timely notifications and forward relevant patch requests to respective OEMs, who respond promptly.

"I have discovered that my incoming bot traffic is agent-based.

"Radware Bot Manager is compliant with my needs, and I do not foresee any problems with it.."

Validated user

Network infrastructure lead at a financial services firm with 501-1,000 employees

Read full review

©2026 PeerSpot, All Rights Reserved

“The best features that Radware Cloud WAF Service offers are DDoS attack and bot mitigations, which stand out as the most significant use cases since we have faced multiple DDoS attacks during and after implementations and also the activities from bots.

“The DDoS attack mitigation and bot mitigation have worked well for us, as we implement rate limits to requests and block connections from countries like China where we don't have clients, which has helped us to identify and block these attacks.

“I have used the API Discovery feature, which Radware Cloud WAF Service helped us identify multiple APIs that we were not aware of in our legacy applications.

“I find API Discovery to be quite easy to use because the Radware Cloud WAF Service support team assisted us in implementing this feature, and it allows for discovery within an hour.

“As of now, we haven't encountered any zero-day threats, but I assume Radware Cloud WAF Service would help us block such threats.

“We are using the automated source blocking feature, and we've had a good experience blocking connections from places like China with the policies we've created.

“The automated source blocking feature has effectively protected our interconnected applications by blocking connections based on identified malicious IPs.

“We are using Radware Bot Manager, though I haven't managed it much as the support team enabled the features and policies.

“After implementing Radware Bot Manager, we discovered multiple APIs being flagged as bots due to regular database queries, which we identified and resolved over time.

“Automated analytics are good features of Radware Cloud WAF Service, enabling us to identify multiple events in a single dashboard and troubleshoot issues effectively.

©2026 PeerSpot, All Rights Reserved

"The real-time BLA detection and mitigation features help us to mitigate threats effectively.

"The combination of negative and behavioral-based positive security models is crucial for our security strategy, as they learn connection behaviors to block unusual activities.."

Yogesh Dayma
Assistant Director Of IT at a non-profit with 1,001-5,000 employees

Read full review

©2026 PeerSpot, All Rights Reserved

“I consider the best feature that Radware Cloud WAF Service offers is protection against application layer attacks, layer seven, mainly.

“That layer seven protection has benefited me significantly by reducing false positives and guaranteeing service availability for us.

“I have positive impressions of the API Discovery feature, since it allows me to discover APIs. The API Discovery feature has helped me register some APIs that I didn't have, and it has also made it easier for me in my integrations with other services. It has seemed a very useful and easy-to-use functionality given its platform.

“I would rate Radware Cloud WAF Service's ability to protect against zero-day attacks as very effective, since recently, given the PHP vulnerability, it helped us to mitigate that type of attack until we carried out patching and mitigation.

“I use the automatic source blocking feature in Radware's cloud application protection solution, and the experience has been very good, as the functionality helps us in the detection and protection of applications.

“The proactive and holistic approach based on correlation between modules has been effective in protecting my applications since, as the modules are from the same vendor, they allow us more native integration and they operate more efficiently.

“My opinion of the automated analytics for event review that the platform offers is positive, as sending metrics on a monthly basis in order to optimize our services, and the automated analytics helps us provide that report.

“I would rate Radware Cloud WAF Service's ability to block unknown threats and attacks as very good, as it allows us to block unknown threats and attacks thanks to its knowledge base.

“I consider the combination of negative and positive security models based on behavior important for my organization's security strategy, since attackers are constantly evolving and modifying IOCs, which challenges us to use this kind of behavioral analysis for more efficient detection.

©2026 PeerSpot, All Rights Reserved

“I consider that Bot Manager would help in my compliance efforts, since the reports we are requested are quarterly, mainly for regulatory compliance that we have.

“Regarding Radware Cloud WAF Service's artificial intelligence capabilities, I think its governance and security level seem appropriate.

“The accuracy and reliability of the results offered by the platform's artificial intelligence convince me, since the AI helps us automate some processes and searches..”

Carla Vega

Defensive cybersecurity engineer at a financial services firm with 1,001-5,000 employees

Read full review

©2026 PeerSpot, All Rights Reserved

"The standout features of Radware Cloud WAF Service are automated attack prevention, bot protection, DDoS mitigation, behavioral analytics, and easy cloud-based deployment. These capabilities help strengthen application security while minimizing manual effort and maintaining application performance.

"Real-time threat detection and automated protection are the features I rely on most in my day-to-day operations. They proactively block web attacks with minimal manual effort, provide clear visibility into malicious activity, and help ensure applications remain secure and available.

"One additional aspect worth highlighting about Radware Cloud WAF Service is the usability and integration capabilities of the platform. The user interface is intuitive and provides a centralized view of attacks, blocked requests, traffic trends, and security events, making day-to-day monitoring straightforward. I also benefit from the integration with SIEM and security monitoring tools, which helps correlate WAF events and other security logs for faster incident investigation and response.

"The capabilities of Radware Cloud WAF Service help improve threat detection and reduce false positives by identifying unusual traffic patterns and emerging attacks. From a governance and security perspective, it provides good visibility and control, allowing security teams to review and validate AI-driven decisions. Overall, the AI features enhance security operations while maintaining transparency and oversight.

"Radware Cloud WAF Service is generally accurate and reliable in identifying malicious traffic, bot activity, and behavior patterns. In my experience, AI helps reduce false positives and improve detection compared to traditional rule-based approaches alone. While occasional tuning may be required for a specific application, the overall accuracy and consistency of the AI-driven insights have been effective for day-to-day security operations.

"Radware Cloud WAF Service is highly effective in blocking unknown threats because it uses behavioral analysis, user learning, and anomaly detection rather than relying solely on predefined signatures. This allows me to identify and mitigate suspicious activity even when the attack pattern has not been seen

©2026 PeerSpot, All Rights Reserved

before. For example, I observed automated traffic targeting a login API from multiple IP addresses using an unusual request pattern. Although the traffic did not match a known signature attack, Radware Cloud WAF Service identified the abnormal behavior, flagged it as suspicious, and automatically applied mitigation controls. This helped prevent potential credential stuffing and bot attacks without impacting legitimate users. Overall, its ability to detect and respond to previously unknown threats has improved my confidence in protecting web applications and APIs against evolving attack techniques.

“The automated analytics of Radware Cloud WAF Service are one of the strongest aspects of the solution. They provide clear visibility into attack threats, malicious traffic, and security events in real-time, making it easier to identify threats and prioritize investigation. The dashboards and automated insights help reduce manual analysis effort and enable faster incident response.

“I use the API discovery feature, which helps identify and inventory my APIs..”

Abhishek Gurav
Cybersecurity Engineer at a financial services firm with 201-500 employees

Read full review

©2026 PeerSpot, All Rights Reserved

Other Solutions Considered

"We were previously using other services before Radware Cloud WAF Service because we have a better relationship with Radware, so currently we are using Radware Cloud WAF Service.."

Sachin Verma
Sr. Neetwork and security Engineer at a outsourcing company with 201-500 employees

Read full review

"Other options in the market were evaluated, looking at different alternatives from different vendors. Palo Alto and Check Point were evaluated before deciding on Radware Cloud WAF Service.."

Roberto Carlos Castellar Ardila
Coordinador de Innovacion Tecnologica y SAP at Expreso Brasilia

Read full review

"We did not switch from a different solution, as we previously used F5. During our evaluations for Radware Cloud WAF Service, we found it to be a good solution to augment our existing security with capabilities around application protection, DDoS, bot and API security visibility, SIEM integration, and operational efforts.."

Validated user
Senior Manager, Cloud Infra & Security at a insurance company with 201-500 employees

Read full review

©2026 PeerSpot, All Rights Reserved

"We previously used another security solution. We decided to move away from it because it did not meet our expectations, particularly regarding its cloud-based capabilities. We are more satisfied with Radware Cloud WAF and would recommend it over the previous solution, especially for cloud-based web application protection.."

Validated user

Read full review

Department of Protection Control of Information & Communication Systems Head at a financial services firm with 1,001-5,000 employees

"Before choosing Radware Cloud WAF Service, we evaluated multiple products for comparison.

"We evaluated Akamai WAF before choosing Radware Cloud WAF Service, which has proven to be stable in our experience.."

Yogesh Dayma

Read full review

Assistant Director Of IT at a non-profit with 1,001-5,000 employees

©2026 PeerSpot, All Rights Reserved

"Before choosing Radware Cloud WAF Service, we evaluated other options from Cisco and we considered Cloudflare.

"I chose Radware Cloud WAF Service instead of the other option after doing a pilot, and the results were much better and more convincing in terms of what we expected regarding the impact of the tool on our platform.."

Armando Rodríguez
Gerente de Tecnologia at Expreso Brasilia

Read full review

©2026 PeerSpot, All Rights Reserved

ROI

Real user quotes about their ROI:

"I have seen a clear return on investment; the main return I could mention is the time it has allowed us to save so we can allocate it to other projects.."

Carla Vega

Defensive cybersecurity engineer at a financial services firm with 1,001-5,000 employees

Read full review

"Initially, I purchased 30 licenses for Radware Cloud WAF Service, expecting to protect only my internet-facing applications. However, impressed by its performance, I have since increased my licenses to 91, reflecting my satisfaction and need for enhanced security.."

Validated user

Network infrastructure lead at a financial services firm with 501-1,000 employees

Read full review

©2026 PeerSpot, All Rights Reserved

"Since using Radware Cloud WAF Service, we have seen positive value from the solution, particularly through improved security coverage, centralized monitoring, and reduced manual effort.."

Validated user

Senior Manager, Cloud Infra & Security at a insurance company with 201-500 employees

Read full review

"I have seen a return on investment since I started using Radware Cloud WAF Service through time savings. We now have all the traffic and visibility centralized for what goes to our exposed applications, allowing us to save time when reviewing all the traffic.."

José Chamorro

Analista de Infraestructura at Expreso Brasilia

Read full review

"Since I started using the platform, one specific result that has improved is the reduction in the number of unauthorized access attempts, which is good because we are in the process of ISO 27001 certification, and this has decreased considerably. Additionally, the impact on response times and process optimization has been excellent, as response times have decreased considerably and our platform has higher levels of availability.."

Armando Rodríguez

Gerente de Tecnologia at Expreso Brasilia

Read full review

©2026 PeerSpot, All Rights Reserved

"API Discovery has helped us reduce overhead costs by roughly 20 to 30% by identifying data transitions.

"By implementing Radware Cloud WAF Service, we are able to reduce the number of employees needed for security, providing indirect savings for the organization.."

Yogesh Dayma
Assistant Director Of IT at a non-profit with 1,001-5,000 employees

Read full review

©2026 PeerSpot, All Rights Reserved

Use Case

"My main use case for Radware Cloud WAF Service is to prevent attacks. We have web applications for our company, and we need to prevent those web apps from various kinds of attacks such as DDoS or injection attacks.."

YogeshTalekar
Associate at Mirae Asset Capital Markets (I) Pvt Ltd

Read full review

"Radware Cloud WAF Service is primarily used to protect our web applications. We have various kinds of applications related to trading apps and our company web app, so we need to protect them from DoS and DDoS web attacks. For those main applications and managing the traffic for those applications, we are using Radware Cloud WAF Service. With this service, we have successfully mitigated some DoS attacks and some DDoS attacks, and we have prevented some attacks as well by blocking some IPs and implementing country geo-blocking. Geo-blocking is the most helpful feature from Radware Cloud WAF Service.."

ShripadMahurkar
Assistant Manager, Information Security Department at Mirae Asset Capital Markets (I) Pvt Ltd

Read full review

©2026 PeerSpot, All Rights Reserved

“My main use case for Radware Cloud WAF Service is securing our applications, as all my applications are public-facing applications, to secure them from the latest and known web threats, since web attacks are a common thing today.

“One application I'm protecting with Radware Cloud WAF Service is the Donor Management System, as we deal with donor's data, and we must ensure that all the data in our servers and applications are secured, especially with DPDP being in full force in India, so WAF helps in securing that data and provides bot support for DDoS attacks.

“Radware Cloud WAF Service helps us because we are dealing with children's and donor's data, and since the applications are public-facing, we must ensure the safety of both the data and the applications..”

Yogesh Dayma
Assistant Director Of IT at a non-profit with 1,001-5,000 employees

Read full review

©2026 PeerSpot, All Rights Reserved

"Radware Cloud WAF Service protects my internet-facing web applications and APIs from cyber threats such as SQL injection, cross-site scripting, bot attacks, DDoS attacks, and other OWASP vulnerabilities. I use it to continuously monitor and filter malicious traffic, ensure application availability, security, and compliance while reducing the risk of data breaches and service disruptions.

"Radware Cloud WAF Service secures my customer-facing web application. For example, I use Radware Cloud WAF Service to secure public-facing applications by blocking SQL injection and XSS attacks and protecting the login API from bot-driven abuse and malicious traffic.

"The challenge Radware Cloud WAF Service addresses is its unique ability to mitigate automated bot attacks and malicious scanning while maintaining a seamless user experience. It reduced operational overhead, improved visibility into web threats, and helped ensure uninterrupted access to critical applications and APIs.."

Abhishek Gurav
Cybersecurity Engineer at a financial services firm with 201-500 employees

Read full review

©2026 PeerSpot, All Rights Reserved

“My main use case for Radware Cloud WAF Service is for cloud security.

“I have onboarded approximately 71 applications, and Radware Cloud WAF Service is for app protections and bot and API protections. It is working flawlessly and provides me with a summary report that is very useful for viewing monthly logs, weekly logs, attack information, bot information, and signature-based, attack-based, and malicious-based information.

“I use Radware Cloud WAF Service every day to monitor for any sort of spike. I have DDoS services and web DDoS services, and if there is a spike, I collect the IP information and broadcast this IP address to other environments to block it. It is extremely useful for identifying malicious IP addresses. It mostly protects my application, and I am very happy with this product.

“I enable Bot Manager across all applications..”

Validated user

Network infrastructure lead at a financial services firm with 501-1,000 employees

Read full review

©2026 PeerSpot, All Rights Reserved

"The main use case I have for Radware Cloud WAF Service is protection against attacks, bots, and automated attacks that target our technology infrastructure.

"I use this tool as the first line of defense, since it allows me to filter, monitor, and block traffic when it detects these types of automated attacks and bots.

"The main use case works very well, and the technical support and alerts are early. If updates are made, they are also reported in a timely manner.

"I use the CDN services offered by Radware along with Radware Cloud WAF Service, which help us to deliver the services we have much more efficiently, given their multinational deployment.

"I use protection against DDoS attacks at layer 7, HTTP/L7, specifically Radware DefensePro, which is an on-premise solution, and it helps us stop denial-of-service attacks that could be carried out.."

Carla Vega

Defensive cybersecurity engineer at a financial services firm with 1,001-5,000 employees

Read full review

©2026 PeerSpot, All Rights Reserved

Setup

The setup process involves configuring and preparing the product or service for use, which may include tasks such as installation, account creation, initial configuration, and troubleshooting any issues that may arise. Below you can find real user quotes about the setup process.

"The configuration has been very easy, we have not had any issues, and when acquiring the license, it is released very easily at the time of purchase and thus protects the sites.."

Nixon Lagos

Jefe especialista de ciberseguridad at a insurance company with 1,001-5,000 employees

Read full review

"Cloud WAF's ability to integrate with other systems and applications in our environment has a normal onboarding process that presents no difficulties in onboarding any applications onto Radware.."

Vishal Salve

manager at a financial services firm with 201-500 employees

Read full review

©2026 PeerSpot, All Rights Reserved

"The implementation actually depends on the requirements of the customers and how many applications there are to be protected. It will only take a couple of hours, or maybe an hour, to implement the initial setup. It is up to the customer to add applications that they want to protect.."

RaynielBadiola

Technical Director at Secur Links

Read full review

"My experience with pricing, implementation costs, and licensing is positive, as the costs were quite well adjusted, the cost-benefit ratio is very good. The implementation also had a very reasonable cost and the timelines were excellent, with no major delays or setbacks, and the results were seen almost immediately.."

Armando Rodríguez

Gerente de Tecnologia at Expreso Brasilia

Read full review

©2026 PeerSpot, All Rights Reserved

"It has been easy for me to integrate the CDN services with Radware Cloud WAF Service, and we did not encounter any challenges during the integration thanks to the documentation it has.

"I would rate the integration of Radware Cloud WAF Service with other systems and applications in my environment as easy due to the amount of documentation and support they have.."

Carla Vega

Defensive cybersecurity engineer at a financial services firm with 1,001-5,000 employees

Read full review

©2026 PeerSpot, All Rights Reserved

"We currently use the integrated WAF option on the same device in our application (SBI). There is no dedicated WAF solution. There are two options: license-based and integrated. Using the integrated part helps to identify blocks and other issues effectively.

Integrating with other systems and applications in the environment:

Integration is not difficult. In the dashboard, under the policy section, we can find virtual services and easily enable the API service. Once enabled, WAF monitoring should also be enabled. We can then identify the application's requirements, like JSON ID, cookies, headers, what should be whitelisted, body size, etc.

We can gather this information from the application owner during deployment to determine what needs to be whitelisted, such as extensions, zip files, XML files, and cookies.

Once we deploy an application, it doesn't take too much time because the application is already deployed. We also use the load balancing feature, so we just need to enable the security web application service. There is an option for this under virtual services where we can also enable it for bot protection. I think anyone can easily manage it if they know about these things.

Radware is signature-based. The patches and signatures are important because we cannot easily monitor them ourselves. They are regularly updated, I think, weekly, so that's helpful. I think this regular update makes it easier for us.."

Gaurav_Mishra

Senior Security Consultant at kyndryl

Read full review

©2026 PeerSpot, All Rights Reserved

Customer Service and Support

"I find Radware Cloud WAF Service's customer support to be good. I rate the customer support of Radware Cloud WAF Service a ten on a scale of one to ten.."

Validated user
Lider Ciberseguridad at a consumer goods company with 201-500 employees

Read full review

"The customer support is good compared to other web services from other vendors, and our TAC team provides remote support and resolves my queries on time and within SLA.."

Sachin Verma
Sr. Neetwork and security Engineer at a outsourcing company with 201-500 employees

Read full review

"Customer support for Radware Cloud WAF Service is good and they are available within a small time limit. I would rate the customer support for Radware Cloud WAF Service an eight.."

Vishal Salve
manager at a financial services firm with 201-500 employees

Read full review

©2026 PeerSpot, All Rights Reserved

"Radware Cloud WAF Service's customer support operates with defined SLAs, responding promptly based on priority levels. They provide thorough guidance, escalating issues as needed and ensuring I am informed of resolutions.

"I rate customer support for Radware Cloud WAF Service a perfect 10.."

Validated user

Network infrastructure lead at a financial services firm with 501-1,000 employees

Read full review

"It's software-only, so most of the time it works as intended. However, I did raise one request about a filter option in the dashboard not working perfectly. We identified that there was a version issue, and they fixed it in a new patch. They were able to easily identify and resolve the version issue.

They are not globally available but can manage and support us within a range of five to seven. They can usually provide support easily.."

Gaurav_Mishra

Senior Security Consultant at kyndryl

Read full review

©2026 PeerSpot, All Rights Reserved

"I have contacted the technical support of Radware twice in three years when we needed some configuration.

"My experience with the quality of the support and the speed of response was quick.

"I think the quality of the support is good. It is a good service.

"If I were to rate them on a scale from one to ten, I would give the support a score of ten.."

Julio Galarza

Coordinador Nacional De TIC Y Sistemas De La Universidad Catlica Boliviana San Pablo at Bolivian Catholic University

Read full review

©2026 PeerSpot, All Rights Reserved

Other Advice

"I have played multiple roles while using Radware Cloud WAF Service, sometimes as a developer, sometimes as a designer, and also involved in application architecture. On a scale of one to ten, I rate Radware Cloud WAF Service a ten because I believe it is a perfect tool. Our organization engages with Radware Cloud WAF Service closely while deploying other public-facing applications using Radware Cloud WAF Service.."

Validated user
Solution designer at a government with 10,001+ employees

Read full review

"I would rate Radware Cloud WAF Service overall as a nine out of ten. I give it a nine because it delivers strong protection against web application attacks, provides effective bot mitigation, and overall things are handled well. If these enhancements were available, especially more customizable analytics and broader native integrations, it would likely be a ten out of ten solution for my organization. Overall, Radware Cloud WAF Service is a reliable and mature WAF platform that effectively addresses web application security requirements.."

Abhishek Gurav
Cybersecurity Engineer at a financial services firm with 201-500 employees

Read full review

©2026 PeerSpot, All Rights Reserved

"I give Radware Cloud WAF Service a rating of nine out of ten.

"I give it a nine because the pricing poses a challenge for us.

"I would advise others to consider using Radware Cloud WAF Service, as we are quite happy with the services.."

Yogesh Dayma
Assistant Director Of IT at a non-profit with 1,001-5,000 employees

Read full review

"I would rate Radware Cloud WAF Service a perfect 10.

"I chose 10 because I was initially looking for a product that provides the best security features, and Radware Cloud WAF Service delivers so many options, allowing me to select what is relevant for my needs. They continually update their database to address emerging threats, which is why I rate it so highly.

"Radware Cloud WAF Service is deployed in my organization via a public cloud.."

Validated user
Network infrastructure lead at a financial services firm with 501-1,000 employees

Read full review

©2026 PeerSpot, All Rights Reserved

"Radware Cloud WAF Service is deployed in my organization in the public cloud.

"We use the provider's SaaS service to deploy Radware Cloud WAF Service.

"We are currently not using the hardware Bot Manager.

"My advice to others who are considering using Radware Cloud WAF Service is to opt for this option, since it has provided us with very positive results.."

Carla Vega
Defensive cybersecurity engineer at a financial services firm with 1,001-5,000 employees

Read full review

"Overall, I am rating Radware Cloud WAF Service as a nine. It is a good product, but it is not perfect, as I have told you about the improvements needed for this tool. Although it is a good tool, that is why I am giving it a nine.

"I have not quite used the AI capabilities of Radware Cloud WAF Service as of now, but I will use it and then provide feedback.

"Radware Cloud WAF Service is a good service that can be used with AI upgradation. Customer support is pretty good, and it can mitigate unnecessary traffic and prevent DDoS or bot attacks mostly. It is a pretty good tool to use for web apps.."

YogeshTalekar
Associate at Mirae Asset Capital Markets (I) Pvt Ltd

Read full review

©2026 PeerSpot, All Rights Reserved

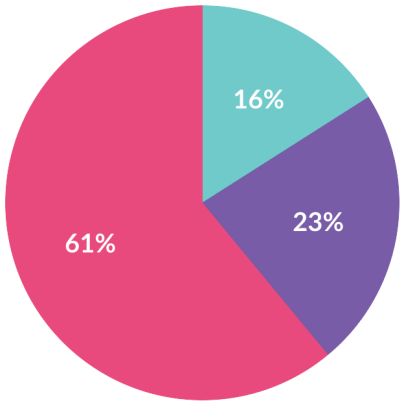
Top Industries

by visitors reading reviews

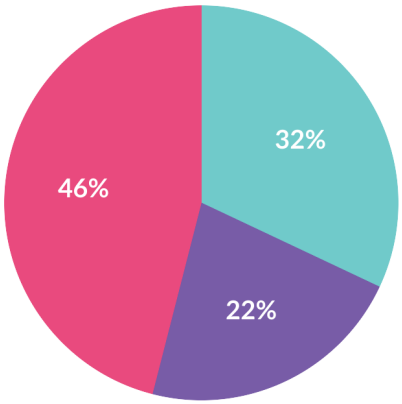
Financial Services Firm	19%
Manufacturing Company	15%
Energy/Utilities Company	14%
Computer Software Company	6%

Company Size

by reviewers



by visitors reading reviews



Large Enterprise Midsize Enterprise Small Business

©2026 PeerSpot, All Rights Reserved

About this buyer's guide

Thanks for downloading this PeerSpot report.

The summaries, overviews and recaps in this report are all based on real user feedback and reviews collected by PeerSpot's team. Every reviewer on PeerSpot has been authenticated with our triple authentication process. This is done to ensure that every review provided is an unbiased review from a real user.

Get a custom version of this report... Personalized for you!

Please note that this is a generic report based on reviews and opinions from the collective PeerSpot community. We offer a customized report of solutions recommended for you based on:

- Your industry
- Company size
- Which solutions you're already considering

The customized report will include recommendations for you based on what other people like you are using and researching.

Answer a few questions in our short wizard to get your customized report.
Get your personalized report here

©2026 PeerSpot, All Rights Reserved

About PeerSpot

PeerSpot is the leading review site for cloud, AI, and business software. We created PeerSpot to provide a trusted platform to share information about software, applications, and services. Since 2012, over 22 million people have used PeerSpot to choose the right software for their business.

PeerSpot helps tech professionals by providing:

- A list of products recommended by real users
- In-depth reviews, including pros and cons
- Specific information to help you choose the best vendor for your needs

Use PeerSpot to:

- Read and post reviews of products
- Access over 30,000 buyer's guides and comparison reports
- Request or share information about functionality, quality, and pricing

Join PeerSpot to connect with peers to help you:

- Get immediate answers to questions
- Validate vendor claims
- Exchange tips for getting the best deals with vendor

Visit PeerSpot: www.peerspot.com

PeerSpot

244 5th Avenue, Suite R-230 • New York, NY 10001

reports@peerspot.com

+1 646.328.1944

©2026 PeerSpot, All Rights Reserved