



Radware DDoS

Reviews, tips, and advice from real users



Powered by  **PeerSpot**

Contents

Product Recap..... 3 - 4

Valuable Features..... 5 - 12

Other Solutions Considered..... 13 - 15

ROI..... 16 - 18

Use Case..... 19 - 22

Setup..... 23 - 25

Customer Service and Support..... 26 - 28

Other Advice..... 29 - 33

Trends..... 34 - 35

About PeerSpot..... 36 - 37

Product Recap



Radware DDoS

Radware DDoS Recap

Radware DDoS provides robust multi-layer protection against distributed denial of service attacks, featuring real-time monitoring and anomaly detection. Its scalable cloud-based and on-site deployment options ensure effective safeguarding of critical infrastructure.

Offering comprehensive defense, Radware DDoS includes features like data scrubbing, signature updates, and SSL-based mitigation. Integrated platforms and a user-friendly interface streamline its deployment. With advanced reporting, analytics, and behavioral analysis powered by machine learning, users experience fewer false positives. Despite these strengths, users highlight the need for improved scalability, seamless deployment, and enhanced machine learning capabilities. Better documentation, pricing, and customer service remain areas of improvement.

What features does Radware DDoS offer?

- **Data Scrubbing:** Filters malicious data from incoming traffic.
- **Signature Updates:** Keeps threat signatures current.
- **SSL-Based Mitigation:** Protects against SSL attacks.
- **Auto Mitigation:** Quickly responds to detected threats.
- **Multi-Layer Protection:** Defends across several attack vectors.

What benefits should users expect?

- **Scalable Protection:** Adaptable to increasing demands.
- **Proactive Notifications:** Alerts in real-time to threats.
- **Live Attack Insights:** Provides real-time analytics.
- **Enhanced Security:** Shields diverse sectors.
- **Reduced False Positives:** Enabled by machine learning.

In industries like banking, telecom, and government, organizations employ Radware DDoS to protect networks from DDoS attacks. It ensures server, web service, and mail security while enabling traffic monitoring and unauthorized access blocking. Its cloud-based options serve entities seeking infrastructure security and network traffic analysis.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- ✓ “Radware DDoS can reduce our bandwidth and provide the required performance, handling SSL encryption, decryption, offloading, compression, DDoS protection, and reverse proxy so that with only four to five servers we are properly optimized, getting excellent two to three millisecond response times and avoiding additional infrastructure investment.”



Verified user

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

- ✓ “After placing this DDoS solution, I do not think we have ever had downtime during this peak of the peak business season.”



Rajesh Bhardwaj

AGM Technology at a newspaper with 5,001-10,000 employees

- ✓ “Radware DDoS is very useful for us in protecting from many attacks, particularly flood attacks and SYN flood attacks, which we deal with in the banking environment.”



Amit Kumar Kurmapu

Technical Specialist at HCLSoftware



“My advice or recommendation to other organizations looking into Radware DDoS is to use it because it is very user-friendly, and we have suggested it multiple times to colleagues and friends due to its comprehensive monitoring capabilities.”



Parag Naik

Cybersecurity Manager at Yotta Infrastructure Solutions LLP



“Radware DDoS has been very good in mitigating advanced DDoS threats, such as burst, DNS attacks, floods, and web scraping, while ensuring that legitimate users are not affected during a DDoS attack.”



RiaanDu Preez

Senior Cyber Security Specialist Architect at a outsourcing company with 11-50 employees



“The best thing about Radware DDoS for me is that the solution is very accurate, the information and the different types of graphics and data are very important, and it is easy to operate and to understand the solution in my case.”



Jhonatan Arturo Abril U.

Professional Consultor Digital Services at a comms service provider with 10,001+ employees



“Radware DDoS has impacted my organization positively by providing robust DDoS protection, offering excellent security and support, and serving as an effective solution that detects attacks and mitigates them, which has allowed us to concentrate on other areas.”



Verified user

Lead Network Reliability Engineer at a comms service provider with 51-200 employees

What users had to say about valuable features:

“In my opinion, the best features Radware DDoS offers are the dashboard, the event visualization, and the use of AI integrated into the tool.

The dashboard and the use of AI for visualization help me in my work because the dashboard makes it very visual for potential events, and the AI is quite user-friendly and useful.

Radware DDoS has positively impacted my organization by helping us avoid going several days without the important application. With Radware DDoS, I can keep our portal applications running for several days without interruption, which enables the institution to continue serving the public..”

Ricardo Salazar Palomino

Analista at a government with 51-200 employees

[Read full review](#)

“The best features that Radware DDoS offers, in my opinion, are the fast detection of attacks and response mitigation. The fast detection and mitigation functions have made a concrete difference in my team's daily operations by allowing us to quickly detect DDoS attacks.

“Radware DDoS has positively impacted my organization by notifying us of attacks that may be carried out against the company, and seeing possible network scans. We have noticed improvements since we detect traffic floods, and that helps us with our daily analysis and alerting about possible incidents..”

Verified user

cyber security expert at a tech services company with 10,001+ employees

[Read full review](#) 

“What I like most about Radware DDoS is a favorite feature that we call a pipe. That is the clean traffic that they guarantee towards our company, our bank. The clean traffic is actually the favorite feature that we have, and that is one of the reasons why we went with Radware instead of other solutions. I also appreciate their responsiveness because we were having some troubles initially to establish the whole traffic and routes. They were very responsive to that and helped us a lot. They essentially did the whole routing traffic and everything by themselves because we did not have engineers with experience in internet routing traffic.

“Radware has been effective at mitigating advanced DDoS threats, such as Burst and DNS attacks. There were several attacks that I was not even aware of. That is actually the best scenario because I did not know that I was attacked, and that demonstrates how effective they are. I think the best answer is when you are not even aware that you are under attack..”

Verified user

[Read full review](#) 

Chief Information Security Officer at a financial services firm with 201-500 employees

“The key benefits I have seen from using Radware DDoS relate to managing 300 customers. I am currently using multiple attacks to figure out, detect, and mitigate properly while providing the proper details, proper traffic flow, and satisfaction to end-user customers. I just protected a 50 to 60 GB attack.

My experience with Radware's behavior-based detection technology in terms of real-time attack detection and minimizing false positives shows that multiple times there are false positive traffic drops. For this reason, we have verified with the particular application team because by default, Radware DDoS is directly using the default policies. We monitor for five to seven days to observe the traffic, and then we set the threshold properly. Multiple times errors and issues show that legitimate traffic can be dropped, as the system is not understanding the particular customer's ports.

We have first analyzed and then set particular policies and thresholds for Radware DDoS for specific customers.

I find Radware DDoS stable.

I find it scalable with no challenges because we are using all technology from Radware. I am not handling another technology..”

Parag Naik

Cybersecurity Manager at Yotta Infrastructure Solutions LLP

[Read full review](#) 

“Radware DDoS has always managed to mitigate the attacks by cleaning all the dirty traffic and keeping the services regularly usable.

“According to my experience, the best features offered by Radware DDoS are the noticeable protection it provides and the ease of use through their portal.

“Radware DDoS's portal has made operational management easier for me as it is very clear, intuitive to use, and simple for performing searches to understand the nature of the block and create any exceptions when necessary. You can periodically request a policy review of the protected sites to analyze all the existing rules and determine whether it is necessary to make any changes, also with the support of Radware DDoS, which obviously has more experience in evaluating the individual rules and suggesting potential changes to be made.

“Radware DDoS has positively impacted our organization by ensuring we have no longer had service disruptions due to attacks of that kind, even though there have been frequent ones over time. Before setting up the service, unfortunately, we suffered some service interruptions and the resulting reputational damage..”

Domenico Cacciari

Security Administrator at regione marche

[Read full review](#) 

“In case of any other general attacks, Radware DDoS actually protects or alerts us. We can configure it as per our requirements, so it will alert us before doing or mitigating things. We can configure it in an auto-protect mode, or we can configure it in an alert mode so that we can go through it and then, accordingly, on the basis of our investigation, determine whether it is the real traffic or the actual attack traffic which we need to mitigate. Legitimate traffic, of course, we need to pass it.

“So sometimes it depends on what policy we have configured. On the basis of that, it will pass the legitimate traffic; sometimes it is a false positive, then we have to go through it and accordingly reconfigure our policy and then from the next time, it will pass the legitimate traffic and will not block. It will mitigate all the DDoS attacks. So it is working well, and every time we face any kind of DDoS attacks, it mitigates them most of the time, 99% of the time, I would say.

“Radware DDoS offers excellent features including a 5 GB capacity box and cloud service benefits. We have taken a Clean Pipe of 200 MB because we have an internet bandwidth of 200 MB. In case of any DDoS attack, because DDoS will choke our internet bandwidth, it will redirect the traffic and then block the DDoS traffic and pass whatever the legitimate traffic is through that 200 MB clear pipe. So we will not face any kind of DDoS, or any attack traffic will be passing through our network.

“The Clean Pipe feature helps our team in real situations by improving the uptime because during a DDoS attack, our bandwidth will be choked out. It will redirect the traffic through that Clean Pipe where only the legitimate traffic will be passed through and the rest, the attack traffic, will be blocked and dropped over the cloud.

“The interface is GUI-based. Most of the things, if we are from the same domain and if we have an understanding of security, basic security features, we would come to know the configuration and how we can configure this. There are only a few things where, because it is the property of Radware, we need their help. But they are one call away, and once we raise the ticket, the tech will be there to help us configure those specific features..”

Rajesh Bhardwaj

AGM Technology at a newspaper with 5,001-10,000 employees

[Read full review](#) 

Other Solutions Considered

“Before choosing Radware DDoS, we evaluated other options like Imperva and F5 due to prices and economic reasons, and I think they decided on this option..”

Verified user

cyber security expert at a tech services company with 10,001+ employees

[Read full review](#) 

“Radware DDoS is the first solution I have used. Earlier, before deploying this solution, I tried only a cloud solution with a local service provider, which is Tata Communication. That was not automated or as good as Radware is. They actually provided the cloud-based solution, and we used it only for three months. After these three months, we moved to Radware DDoS..”

Rajesh Bhardwaj

AGM Technology at a newspaper with 5,001-10,000 employees

[Read full review](#) 

“I have not used any alternatives to Radware DDoS as our system is set up within our premises. However, I was using a system from our internet ISP, and I was not satisfied at all. This was the reason we switched. I believe it was the next day when Russia invaded Ukraine that we were having a major DDoS. All banks in Macedonia were having major DDoS attacks, and the ISP protection did not work at all. They did not react at all..”

Verified user

Chief Information Security Officer at a financial services firm with 201-500 employees

[Read full review](#) 

“I have not used any alternatives to Radware DDoS as our system is set up within our premises. However, I was using a system from our internet ISP, and I was not satisfied at all. This was the reason we switched. I believe it was the next day when Russia invaded Ukraine that we were having a major DDoS. All banks in Macedonia were having major DDoS attacks, and the ISP protection did not work at all. They did not react at all..”

Verified user

Chief Information Security Officer at a financial services firm with 201-500 employees

[Read full review](#) 

“I did not use any other DDoS protection solutions before Radware, also implementing FlowPath for particular DDoS solutions. There is no plan for moving to another technology because we have already managed another solution that is better than Radware.

I evaluated other options previously, managing another solution such as F5 DDoS and Array DDoS, but Radware is working properly, better than those, and provides proper details and analysis. We have no plans to change from Radware..”

Parag Naik

Cybersecurity Manager at Yotta Infrastructure Solutions LLP

[Read full review](#) 

“The key differences, both pros and cons of Radware in comparison to the other DDoS technologies I have managed show that previously we managed online, verifying every traffic coming to Radware DDoS, and now we are using offline Radware DDoS. We are managing traffic through NetFlow and SFlow to monitor it. In the past, we managed one customer, but now we are managing about 1,500 customers. We have multiple workflows and set thresholds for particular rules, and Radware DDoS is providing solutions and details for DDoS..”

Parag Naik

Cybersecurity Manager at Yotta Infrastructure Solutions LLP

[Read full review](#) 

ROI

Real user quotes about their ROI:

“I have seen a return on investment with Radware DDoS, particularly saving time for investigations since we use the statistics and traffic measurements to evaluate traffic, and Radware DDoS gives us the results a bit more ready-made..”

Verified user

[Read full review](#) 

cyber security expert at a tech services company with 10,001+ employees

“In the last year, Radware DDoS has mitigated approximately between 15 and 20 attacks, and previously, the longest downtime we suffered was about 8 hours. After that, this problem no longer occurred..”

Domenico Cacciari

[Read full review](#) 

Security Administrator at regione marche

“The cost-benefit of Radware DDoS has helped us significantly. The cost relative to what it does is very valuable. The quality-to-price ratio compared to the tool is good..”

Verified user

[Read full review](#) 

Coordinador De Infraestructura Ti at a manufacturing company with 1-10 employees

“I have definitely seen return on investment with Radware DDoS. The number of failed requests after implementation reduced drastically.

Radware DDoS has reduced my need for additional infrastructure investments due to DDoS threats..”

RiaanDu Preez

[Read full review](#) 

Senior Cyber Security Specialist Architect at a outsourcing company with 11-50 employees

“When it comes to the return on investment with Radware DDoS, it's hard to discuss in terms of money saved, but we definitely don't need to put as much focus on manually looking at attacks and mitigating them. In terms of cost saving, it has meant staff can work on other areas and improve automation or work on bigger issues such as incidents or future projects..”

Verified user

[Read full review](#) 

Lead Network Reliability Engineer at a comms service provider with 51-200 employees

“I have seen a return on investment with Radware DDoS, because earlier we were having downtime. During that downtime, the likes and the hits on our news sites, on our websites, were missed. It depends on how it is redirecting to other sites where we are charging other people, for example, advertising for and then further redirecting to third-party websites whose ads we have running on our websites. So those would also be missed. Especially the hits we are getting on our websites that also pays us sometimes. The return on investment is good..”

Rajesh Bhardwaj

AGM Technology at a newspaper with 5,001-10,000 employees

[Read full review](#) 

Use Case

“The main use case for Radware DDoS in my organization is configuring the thresholds to mitigate DDoS attacks and protect the infrastructure. I have limited SYN and flood connections to mitigate any traffic poisoning or massive connection attacks..”

Verified user

cyber security expert at a tech services company with 10,001+ employees

[Read full review](#) 

“I use Radware DDoS as DDoS protection with active protection. Our BGP is also transferred to Radware. We also have the WAF, which is a web application firewall, but that is a different matter..”

Verified user

Chief Information Security Officer at a financial services firm with 201-500 employees

[Read full review](#) 

“My main use case for Radware DDoS is for analysis of applications published on the internet.

I can give you a quick specific example of how I use Radware DDoS to analyze an application published online. We detected constant events targeting a new application, which allowed us to improve its security..”

Ricardo Salazar Palomino

Analista at a government with 51-200 employees

[Read full review](#) 

“Our main use case for Radware DDoS is to use infrastructural DDoS protection for our AS, and in addition, we have the web DDoS part for the main institutional sites.

“A recent situation in which we used Radware DDoS to protect our infrastructure occurred during a web DDoS attack on the institutional site in February 2025, and thanks to Radware DDoS's service, we resolved it. From that moment on, there have been other attacks periodically, but always thanks to Radware DDoS's service, we have never again taken a hit. The service did its job, and the attacks have no longer been successful..”

Domenico Cacciari

Security Administrator at regione marche

[Read full review](#) 

“My main use case for Radware DDoS is to eliminate DDoS attacks. Because it is an anti-DDoS solution, we were observing a lot of DDoS attacks on our web servers, especially the public-facing applications. We deployed this solution to eliminate these DDoS attacks from multiple countries.

“Especially during the election we were having in our country, specifically for the UP region, Uttar Pradesh, we faced a lot of DDoS attacks on our web server where we publish the news. Because we are a media company, this was a particularly challenging time. Radware DDoS mitigated these attacks successfully..”

Rajesh Bhardwaj

AGM Technology at a newspaper with 5,001-10,000 employees

[Read full review](#) 

“I am currently working with Radware DDoS, and I have completed multiple projects with Radware already. I had some issues that were highlighted, and R&D fixed them. They have good support and provide proper solutions and fix new version bugs.

I have been working with Radware DDoS for three years, and currently, I am handling the Cyber Controller. Previously, we were managing the DefensePro. Both are good technology and good devices. We are managing the DP20, and we are also managing Radware DDoS Cloud. For three years, we have been handling Radware DDoS Cloud and physical DDoS. Six months ago, I implemented a migration and introduced a new Cyber Controller for my organization.

The key benefits of having the hybrid setup with Radware DDoS include using both setups, where if my premise has high capacity, traffic automatically moves to Radware DDoS Cloud, managing 3 GB traffic in the cloud while handling 16 GB traffic internally in a very good setup for multiple customers..”

Parag Naik

Cybersecurity Manager at Yotta Infrastructure Solutions LLP

[Read full review](#) 

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 deployment was very straightforward. We completed it with Radware Professional Services, which did a great job. There were no objections or remarks..”

Ziga Brus

System Engineer at Bankart d.o.o.

[Read full review](#) 

“The initial deployment was not easy, but with the help of Radware engineers, it was not that difficult. From an engineering point of view, it was interesting. Because we did not have BGP and did not have all the prerequisites that we needed, it was challenging for us engineers. I cannot say that it was easy, but I also cannot say that it was difficult. It was challenging..”

Verified user

Chief Information Security Officer at a financial services firm with 201-500 employees

[Read full review](#) 

“My experience with the deployment was straightforward. Obviously, there were some misunderstandings and assumptions that came to light during the deployment. From my side, that is normal in these situations: not understanding what was explained or someone within the team on our side assuming something instead of asking questions and conducting research..”

RiaanDu Preez

[Read full review](#) 

Senior Cyber Security Specialist Architect at a outsourcing company with 11-50 employees

“We usually receive the alert after an attack. Earlier, during the configuration and setup of this solution, we first configured it as an alert. Later, gradually and over a period of time, we configured it as per our requirements. We understood the traffic pattern, and then accordingly, after taking multiple steps or multiple configurations, we reached this stage where we are mitigating most of the traffic, most of the DDoS traffic, in the first attempt itself..”

Rajesh Bhardwaj

[Read full review](#) 

AGM Technology at a newspaper with 5,001-10,000 employees

“My experience with the deployment of Radware DDoS has been smooth. We had the existing product of Radware, so we only had to export and import the configuration. A half hour of downtime was required. It was smooth, and we never experienced such a wonderful migration with Radware. Within a half hour or within a fraction of time, we exported and imported the new configuration to the new hardware from the old hardware, and it has been working smoothly without any hesitation or issue..”

Verified user

[Read full review](#) 

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

“I would describe the ease of integration of Radware DDoS with other tools or systems that I use in my company as relatively simple, thanks to its compatibility with widely used networking and security standards. Radware DDoS allows integration with firewalls, and in our case we use Fortinet firewalls, and with additional network-level monitoring platforms that we have in the company.

“Regarding daily management, I would describe the ease of administration and monitoring of Radware DDoS as very good as the dashboard is very intuitive and easy for the end user..”

José Chamorro

[Read full review](#) 

Analista de Infraestructura at Expreso Brasilia

Customer Service and Support

“Whenever a DDoS attack is happening, your team rectifies the situation for us, and that is the main thing for us as a particular metric we have seen since using Radware DDoS..”

Vishal Salve

manager at Miraeassetcm

[Read full review](#) 

“The customer support of Radware DDoS is rated 10 out of 10 because they are always available. We have a customer engagement member always available for us, so if we ever have an incident we're having trouble with or issues with the platform, we can always contact them. They are always on hand and put in the hours to solve any issues..”

Verified user

Lead Network Reliability Engineer at a comms service provider with 51-200 employees

[Read full review](#) 

“I would describe the attention and assistance I have received from the Radware DDoS team as excellent, as they have been there when we have needed them.

“I would describe Radware DDoS's customer support as excellent..”

José Chamorro

Analista de Infraestructura at Expreso Brasilia

[Read full review](#) 

“My experience with Radware DDoS customer support has been excellent.

“I would rate Radware DDoS's response times after an attack as optimal. As soon as the system records and mitigates the attack, Radware DDoS's support service immediately calls to inform us and to ensure that there is no disruption..”

Domenico Cacciari

Security Administrator at regione marche

[Read full review](#) 

“I have contacted the technical support and customer support during attacks. We were having some problems during a DDoS attack when legitimate traffic started to be killed. I contacted them and they immediately resolved the issue. They explained what the problem was, remapped everything about the thresholds, and everything was perfect after that because this was the first time we were experiencing such a type of DDoS attack.

“If I were to rate the technical support on a scale from one to ten, I would give them a nine..”

Verified user

[Read full review](#) 

Chief Information Security Officer at a financial services firm with 201-500 employees

“I assess the cost versus value of Radware DDoS protection compared to other solutions as high, giving it a rating of ten out of nine, with the support-related aspect needing improvement. There are critical drawbacks with customer care, particularly regarding ticket responses.

My impressions of the SecOps dashboards for monitoring and reporting metrics show that the Cyber Controller is probably a very good solution with detailed definitions and reporting.

On a scale of one to ten, I would rate the customer service and technical support of Radware DDoS at seven..”

Parag Naik

[Read full review](#) 

Cybersecurity Manager at Yotta Infrastructure Solutions LLP

Other Advice

“I do not have specific metrics or numbers right now regarding reduced downtime or fewer incidents after using Radware DDoS. I gave this product a rating of 10..”

Ricardo Salazar Palomino

Analista at a government with 51-200 employees

[Read full review](#) 

“I would advise other people who are considering using Radware DDoS that it is a very good tool, that it can be easily implemented, that support is very collaborative, and I would encourage them to try it. I gave this review a rating of 9..”

Verified user

cyber security expert at a tech services company with 10,001+ employees

[Read full review](#) 

“My advice or recommendation to other organizations looking into Radware DDoS is to use it because it is very user-friendly. We have suggested it multiple times to colleagues and friends due to its comprehensive monitoring capabilities. I would rate this product nine out of ten..”

Parag Naik

Cybersecurity Manager at Yotta Infrastructure Solutions LLP

[Read full review](#) 

“Radware DDoS seems to be a complete product, offering a variety of modular sub-services, and so far, we have not had any particular need to ask for changes or new implementations.

“I recommend organizing a POC to test the reliability of the service firsthand to dispel any doubts for others who are considering using Radware DDoS.

“I have provided a comprehensive review of Radware DDoS, and I rate this solution a 10 out of 10..”

Domenico Cacciari

Security Administrator at regione marche

[Read full review](#) 

“When I scheduled the call, it did not allow me to pick a time zone. I was only given time slots to choose from.

“I am familiar with the pricing because I handled the whole procurement, and I think it is fair pricing. Radware is not at the level of [Akamai](#), but they are more expensive than other competition. However, the services that they are providing are on the next level from their competition, and we do not even consider other

providers.

“As of right now, after I deployed it, it does not require any maintenance on my end. I do not connect for maintenance, and I do not believe that our engineers connect either. There may be some preventive maintenance, but it is not heavy and not excessive.

“I have not used the web DDoS protection. My overall rating for Radware DDoS is nine out of ten..”

Verified user

Chief Information Security Officer at a financial services firm with 201-500 employees

[Read full review](#) 

“Radware DDoS has positively impacted my organization, especially during the festive season when we have the peak of the peak business season, during peak seasons like Holi and Diwali. During these days, earlier we were having many DDoS attacks, and during that time, most of the time our website actually went down. After placing this DDoS solution, I do not think we have ever had downtime during this peak of the peak business season.

“Other than festivals, we have this election going on in multiple states in our country. Earlier, when we were not having this particular solution in place, we were facing a lot of downtime on our websites. But after placing this solution, we do not face any kind of such downtime.

“As per my memory, I can recall it was around 7 to 8 hours of downtime in a month before Radware DDoS was placed. After this solution was implemented, we did not have more than 10 to 15 minutes of downtime because it triggered the Clean Pipe and then blocked all the DDoS traffic and passed through the legitimate traffic.

“Radware DDoS has helped us reduce the number of false positives our organization receives in response to attacks by helping us to configure the box and cloud as per our requirements. During the initial time, it was a lot, around 15% false

positives were there. But later on, after the help from the tech as well as the Radware guys, the local support guys who were the L3 level support, they helped us to configure the box and cloud. We reduced the false positives, and later the alert and the legitimate traffic which was getting blocked was further configured to be passed through the channel. Only the genuine DDoS attacks were dropped after this final configuration.

“Radware DDoS has been effective at mitigating advanced DDoS threats like burst attacks during political events or festival events, which is usually the peak business season for us, especially for the media. I cannot say much about DNS attacks because I have not done a further deep dive on what kind of DNS attacks they were, but burst attacks were there. For encrypted SSL floods, we observed this kind of flood. Not frequently, but a few incidents happened in the past where encrypted SSL floods were there and Radware DDoS was able to block them. I am not aware of whether we faced any kind of IoT attacks in our organization.

“My experience with Radware's behavior-based detection technology in terms of real-time attack detection and minimizing false positives depends on the configuration we are doing and varies from industry to industry. For example, in the media industry, it depends on what kind of traffic we are accepting. In the media industry, there are a lot of contents which we need to allow, which, in normal industry, is not permitted, even over the web. Because we are in the media industry, we need to publish reality, including all these things over the newspaper or on our website's digital content. The behavior-based detection, because of the AI integration, always depends on our configuration and what kind of category we are going to block. We have configured it as per our requirements and we got a good response from the solution.

“My impressions of the SecOps dashboards for monitoring and reporting metrics are positive. We have integrated this Radware DDoS solution with our SIM tool solution. Earlier we were using ArcSight. It was easily integrated with the ArcSight SIM solution. Now we are using a different SIM solution, which is [Sentinel](#). With [Sentinel](#) as well, it was integrated without any problem. For non-technical staff, it will definitely not be easy for a non-security person to use the dashboard. The dashboard will clearly show us how many attacks. General people will correlate related to the attacks and the number of DDoS events and how much traffic was

passed through this clear pass channel. But, in case we want to deep-dive further to understand the chronology of attacks and why traffic was blocked or dropped, then we need some technical understanding of these technical things.

“From the governance point, Radware DDoS is quite good. Actually, we are in the media, and we are not looking up to that much of a governance thing. So, whatever is required as per the country or as per the industry, we are getting it through Radware DDoS. I cannot say anything about it because it depends on the industry to industry and the country to country.

“Radware DDoS is deployed in our organization as a hybrid solution: on-premises as well as over the cloud. Radware is the cloud provider we use for our hybrid deployment. They have pitched in the solution of this cloud solution where they are giving us the clear pipe, a clear traffic pipe. It is through their Radware cloud only. The Radware box which is installed in our premise is blocking or dropping the DDoS attacks on the perimeter itself.

“As per my observation, Radware DDoS detects an incident within a few minutes, most probably within 5 to 10 minutes, and then prevents or mitigates it. Within the next five minutes, it triggers, and then accordingly, if the DDoS attack capacity is more than our bandwidth, then it directs the traffic over this cloud and passes the legitimate traffic.

“I would definitely recommend Radware DDoS to others because it is fulfilling the purpose we purchased this solution for. I give this review a rating of 9 out of 10..”

Rajesh Bhardwaj

AGM Technology at a newspaper with 5,001-10,000 employees

[Read full review](#) 

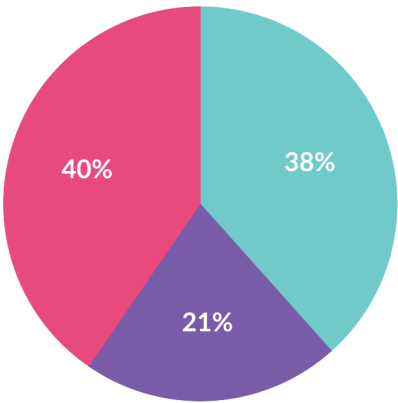
Top Industries

by visitors reading reviews

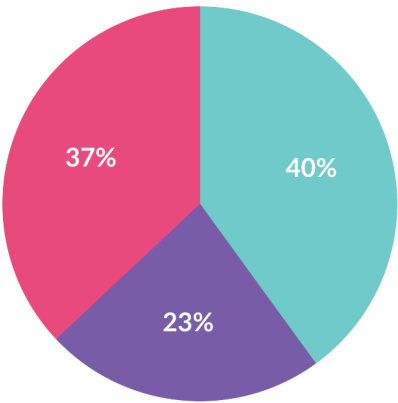


Company Size

by reviewers



by visitors reading reviews



Large Enterprise

Midsize Enterprise

Small Business

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](#)

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