



Arbor DDoS and Radware DefensePro

Product Reviews and Buyer's Guide

September 2018

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

Thanks for downloading this IT Central Station report.

Note that this is a generic report based on reviews and opinions from the entire IT Central Station community. We offer a [customized report](#) personalized for you based on:

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

It includes recommendations for you based on what other people like you are researching and using.

It takes 2-3 minutes to get the report using our shortlist builder wizard. We recommend it!

[Get your personalized report here.](#)

Contents

Overview	4
Top Review by Topic of Arbor DDoS and Radware DefensePro	5
Vendor Directory	6
Top DDoS Vendors, Weighted	7-8
Top 5 Solutions by Ranking Factor	9
About This Report and IT Central Station	10

Overview

SOLUTION



Arbor DDoS



Radware DefensePro

OVERVIEW

Arbor Networks, the security division of NETSCOUT, is driven to protect the infrastructure and ecosystem of the internet. It is the principle upon which we were founded in 2000; and remains the common thread that runs through all that we do today. Arbor's approach is rooted in the study of network traffic. Arbor's suite of visibility, DDoS protection and advanced threat solutions provide customers with a micro view of their network enhanced by a macro view of global internet traffic and...

DefensePro is a real-time, perimeter attack mitigation device that secures organizations against emerging network and applications threats.

Part of Radware's attack mitigation solution, DefensePro protects the infrastructure against network and application downtime (or slow time), application vulnerability exploitation, malware spread, network anomalies, information theft and other types of attacks.

SAMPLE CUSTOMERS

TOP COMPARISONS

[Radware DefensePro vs. Arbor DDoS](#)
Compared 26% of the time

[F5 Silverline DDoS Protection vs. Arbor DDoS](#)
Compared 14% of the time

[Imperva Incapsula vs. Arbor DDoS](#)
Compared 9% of the time

SingleHop

[Arbor DDoS vs. Radware DefensePro](#)
Compared 49% of the time

[Imperva Incapsula vs. Radware DefensePro](#)
Compared 10% of the time

[Check Point DDoS Protector vs. Radware DefensePro](#)
Compared 7% of the time

TOP INDUSTRIES, BASED ON REVIEWERS*

TOP INDUSTRIES, BASED ON COMPANIES READING REVIEWS*

Writing And Editing Position ... 9%
University ... 12%
Recruiting/Hr Firm ... 13%
Comms Service Provider ... 44%

COMPANY SIZE, BASED ON REVIEWERS*

201-1000 Employees ... 20%
1-200 Employees ... 40%
1001+ Employees ... 40%

COMPANY SIZE, BASED ON COMPANIES READING REVIEWS*

* Data is based on the aggregate profiles of IT Central Station Users researching this solution.

Top Reviews by Topic

SOLUTION



Arbor DDoS

ROOM FOR
IMPROVEMENT



Salinda Lekamge

My opinion is that these Arbor devices should be scalable, in terms of the hardware. Network bandwidth is rapidly increasing. Therefore, it is not practical to predict the network traffic as what it will be in five years time and also, to accordingly plan the required hardware specifications. [\[Full Review\]](#)



Radware DefensePro



SolArch9020

From a service provider's point of view, I would like to see better scalability in terms of a platform, rather than sticking to specific models. From a subscription or model-of-operations point of view, I think they should scale it better. In addition, if they would go to a cloud-based approach, that would give much more flexibility in terms of working with them. [\[Full Review\]](#)



DevenderKumar

The auto-mitigation feature is provided when DDoS is observed on any of the links/customers (configured under auto-mitigation). It automatically starts mitigation with the default filters. In the default filter mode, there could be an impact on a customer's link. For example, if we have enabled monitoring of the internal traffic for that link/customer, it starts mitigation on legitimate traffic. It can also create looping in the network for any misconfiguration. This can impact the ISP's internal... [\[Full Review\]](#)



Devender Kumar

Auto mitigation is a feature provided when DDoS is observed on any of link/customer (configured under auto mitigation). It automatically starts mitigation with default filters. In default filter mode, there could be an impact on the customer's link. E.g., if we have enabled monitoring of internal traffic for that link/customer, it starts mitigation on legitimate traffic. It can also creates looping in the network for any misconfiguration, which can impact the ISP's internal network and the custo... [\[Full Review\]](#)

Vendor Directory

A10 Networks	A10 Thunder TPS	Fortinet	FortiDDoS
Akamai	Akamai Kona	Incapsula	Imperva Incapsula
Arbor Networks	Arbor DDoS	Kentik	Kentik
Black Lotus	Black Lotus	Neustar	Neustar DDoS
CDN77.com	CDN77	Nexusguard	Nexusguard
Check Point	Check Point DDoS Protector	Prolexic	Prolexic
Cloudbric	Cloudbric	Radware	Radware DefensePro
Cloudflare	Cloudflare	RioRey	RioRey
Corero	Corero	Shape Security	Shape Security
F5	F5 Silverline DDoS Protection	SiteLock	SiteLock
Fastly	Fastly	Sucuri Security	Sucuri
Flowmon Networks	Flowmon DDoS Defender	Zenedge	Zenedge

Top DDoS Vendors, Weighted

Over professionals have used IT Central Station research. Here are the top vendors based on product reviews, ratings, and comparisons. All reviews and ratings are from real users, validated by our triple authentication process.

Chart Key

● Views	● Comparisons	● Reviews	● Followers	● Average Rating
Number of views	Number of times compared to another product	Total number of reviews on IT Central Station	Number of followers on IT Central Station	Average rating based on reviews

Bar length

The total ranking of a product (i.e. bar length) is based on a weighted aggregate ranking of that product's Views (weighting factor = 17.5%), Comparisons (17.5%), Reviews (17.5%), Followers (17.5%), and Average Rating (30%). Reviews and ratings by resellers are excluded from the rankings. For each ranking factor, the score (i.e. bar segment length) is calculated as a product of the weighting factor and its position for that ranking factor. For example, if a product has 80% of the number of reviews compared to the product with the most reviews in its category, then the product's bar length for reviews would be 17.5% (weighting factor) * 80%.

1 Imperva Incapsula



2 Cloudflare



3 Arbor DDoS



4 Sucuri



5 Radware DefensePro



6 Kentik



3,736 views

1,414 comparisons

4 reviews

239 followers

9.3 average rating

7 SiteLock



8,235 views

4,967 comparisons

1 reviews

187 followers

2.0 average rating

8 Cloudbric



3,061 views

999 comparisons

1 reviews

66 followers

10.0 average rating

9 Prolexic



2,048 views

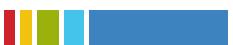
1,250 comparisons

3 reviews

91 followers

8.0 average rating

10 FortiDDoS



1,224 views

691 comparisons

2 reviews

66 followers

10.0 average rating

Top 5 Solutions by Ranking Factor

Views

SOLUTION	VIEWSS
1 Imperva Incapsula	25,051
2 Cloudflare	20,915
3 Arbor DDoS	9,385
4 SiteLock	8,235
5 Sucuri	7,134

Reviews

SOLUTION	REVIEWS
1 Imperva Incapsula	24
2 Cloudflare	15
3 Arbor DDoS	6
4 Kentik	4
5 Prolexic	3

Followers

SOLUTION	FOLLOWERS
1 Imperva Incapsula	703
2 Cloudflare	469
3 Arbor DDoS	370
4 F5 Silverline DDoS Protection	322
5 Sucuri	279

About this report

This report is comprised of a list of enterprise level vendors. We have also included several real user reviews posted on ITCentralStation.com. The reviewers of these products have been validated as real users based on their LinkedIn profiles to ensure that they provide reliable opinions and not those of product vendors.

About IT Central Station

The Internet has completely changed the way we make buying decisions. We now use ratings and review sites to see what other real users think before we buy electronics, book a hotel, visit a doctor or choose a restaurant. But in the world of enterprise technology, most of the information online and in your inbox comes from vendors but what you really want is objective information from other users.

We created IT Central Station to provide technology professionals like you with a community platform to share information about enterprise software, applications, hardware and services.

We commit to offering user-contributed information that is valuable, objective and relevant. We protect your privacy by providing an environment where you can post anonymously and freely express your views. As a result, the community becomes a valuable resource, ensuring you get access to the right information and connect to the right people, whenever you need it.

IT Central Station helps tech professionals by providing:

- A list of enterprise level vendors
- A sample of real user reviews from tech professionals
- Specific information to help you choose the best vendor for your needs

Use IT Central Station to:

- Read and post reviews of vendors and products
- Request or share information about functionality, quality, and pricing
- Contact real users with relevant product experience
- Get immediate answers to questions
- Validate vendor claims
- Exchange tips for getting the best deals with vendors

IT Central Station

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

www.ITCentralStation.com

reports@ITCentralStation.com

+1 646.328.1944