



Akamai Guardicore Segmentation

Reviews, tips, and advice from real users



Powered by  **PeerSpot**

Contents

Product Recap..... 3 - 4

Valuable Features..... 5 - 11

Other Solutions Considered..... 12 - 15

ROI..... 16 - 18

Use Case..... 19 - 21

Setup..... 22 - 25

Customer Service and Support..... 26 - 27

Other Advice..... 28 - 30

Trends..... 31 - 32

About PeerSpot..... 33 - 34

Product Recap



Akamai Guardicore Segmentation

Akamai Guardicore Segmentation

Recap

Akamai Guardicore Segmentation is a software-based microsegmentation solution that provides the simplest, fastest, and most intuitive way to enforce Zero Trust principles. It enables you to prevent malicious lateral movement in your network through precise segmentation policies, visuals of activity within your IT environment, and network security alerts. Akamai Guardicore Segmentation works across your data centers, multicloud environments, and endpoints. It is faster to deploy than infrastructure segmentation approaches and provides you with unparalleled visibility and control of your network.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- ✓ “Guardicore makes its own rule set automatically, so we can work fast when creating a rule set.”



Verified user

Information Security Consultant at a comms service provider with 11-50 employees

- ✓ “Initially, I liked the telemetry part. But later, we used the microsegmentation features that we were able to deploy and found that they really stood out from other vendors. It allows us to see microsegmentation as distributed services.”



Uday Varma

Solution Architect at Inspira Enterprise

- ✓ “The tool's most valuable feature is its visibility.”



Matthias Kropf

Senior Expert Enterprise Architecture at a manufacturing company with 10,001+ employees



“The label-based segmentation is the most valuable feature.”



KlavsThaarup

Senior Security Consultant at Orange Cyberdefense



“The tool is a complete package that offers many features like visibility. You can get a graph with real-time workflows and visibility into server-to-server communication. We get visibility into many things happening within our environment.”



Verified user

Specialist Master - Cyber Risk at a consultancy with 10,001+ employees



“The real bonus is the fact that we can secure applications, all the way down to the individual services, on each host. It's actually more granular security than we can get out of a traditional firewall.”



Joshua Turner

Manager Network & Security Engineering at Teleflora



“The most valuable features of the solution are the maps and ring fencing that help monitor events.”



Ofira Cohen

Analysar at Shaare Zedek Medical Centre

What users had to say about valuable features:

“The tool is easy to use and simple to deploy to achieve segmentation objectives. It offers a graphical view of real-time workflows and traffic patterns into server-to-server communications. Also, the amount of process, service level visibility the agents deployed on the servers provide via network logs is very informative..”

Verified user

[Read full review](#) 

Specialist Master - Cyber Risk at a consultancy with 10,001+ employees

“Guardicore Centra offers the best coverage specifically in backward compatibility with legacy operating systems.

The query insight module is something that our customers found very beneficial.

Creating policies down to a process level on a server is a valuable option.

Integration with Active Directory is good..”

Verified user

[Read full review](#) 

Senior Security Consultant at a tech consulting company with 1,001-5,000 employees

“Initially, I liked the telemetry part. But later, we used the micro-segmentation features that we were able to deploy and found that they really stood out from other vendors.

It allows us to see microsegmentation as a distributed service.

The ease of policy creation and management in Akamai Guardicore Segmentation has impacted security operations. No other product offers more customization. It has some complexity at the initial configuration level, but later on, it becomes easy. If I were to rate it on a scale of ten, I'd give it at least a nine. It is highly mature. .”

Uday Varma

Solution Architechtt at Inspira Enterprise

[Read full review](#) 

“The limitation of security groups, in terms of the number of services you can open that you can cover by using these tools, is great.

If you treat your network as a flat, and then you start creating all your, let's say, network security zones using this tool, it makes life easy. For example, you have always flexibility in having different production and management interfaces.

With a cloud-native construct, you can do micro-segmentation.

The initial setup is easy.

The solution scales well.

I found the solution to be stable. .”

Vishal Chaudhary

Senior Principal Consultant Cloud/DevOps/ML/Kubernetes at Opticca

[Read full review](#) 

“I like the visibility of the communication, so that we really see which communications the assets have to the other assets. We don’t need a further sensor or firewall to see the traffic to these devices. That’s the main reason.

And Guardicore makes its own rule set automatically, so we can work fast when creating a rule set. We don’t have a long phase of monitoring or whatever, so we can go straight to rules where we drop unwanted data traffic.

We don’t do micro-segmentation for each asset. We work with the ring-fencing function, and we have really good visibility on the dashboard with the rings. We can see which asset is in which segment, zone, or ring. That’s the main thing, that we can see this really easily.

We can also give this view not only to the administrator of the Guardicore components but also to the application owner, so they can see where their application is placed in the ring-fencing and what communication is there. This makes incident management easier because we get incidents in a more authenticated way from the application owner. That’s also a big benefit from the visibility of the Guardicore solution.

In the firewall, only the administrator has a deep look into the architecture, the logs, and the segmentation. In the Guardicore solution, we can give more visibility to the application owner on their own application. This makes it easier to manage incidents and the overall management of the application and network. The application owner has a view of the actions happening on the network with their assets or applications..”

Verified user

[Read full review](#) 

Information Security Consultant at a comms service provider with 11-50 employees

“The most valuable feature is the visibility of processes and connections. In addition to the defense it provides, Guardicore gives us a view of each connection that exists on each server. Using this, we can identify things like unused connections, or processes that are using too much in terms of resources. Knowing this, we have the opportunity to block such connections and in turn, improve server performance.

Guardicore supports the operating systems that we require. Primarily, it covers our Microsoft platform, but we have some Linux systems as well. We also used it to protect our SAP HANA database.

I have not compared the range of operating systems that it supports to its competitors because of our use case. We are most interested in LAN segmentation, in particular between the data center and the users' network, so I compared it with other solutions in that context.

It is a benefit that Guardicore supports legacy operating systems, and I have used it with such servers. However, in the long term, it is more important that I have something protecting my data center and having the visibility of what endpoint is initiating connections.

We use the AI-powered segmentation functionality and it affects the time required to design by a lot. It gives us a large number of views and without that, you cannot design the system properly. The AI helps because it shows you what you need to do. Without the AI, either you will not be able to implement the system, or it will take a long time and be very difficult. For us, using this feature saved us a couple of months in implementation time..”

Ehud Huminer

CTO at a consumer goods company with 501-1,000 employees

[Read full review](#) 

Other Solutions Considered

“Akamai is much better than other solutions, such as ColorTokens and Illumio. It is more user-friendly and has more features. In fact, Illumio is actually implementing a lot of the features that Guardicore has had for years..”

KlavsThaarup

Senior Security Consultant at Orange Cyberdefense

[Read full review](#) 

“Guardicore Centra provides better value for money than NSX, was the other solution that we looked at, which was too expensive for what it does. The main difference was that Guardicore just concentrated on segmentation. NSX was more of a network solution that did too many things, and we really didn't need all this stuff that it was doing..”

Verified user

Corporate Operations Manager at University of Strathclyde

[Read full review](#) 

“This product did not replace a similar system. Also, I did not require human resources for this same task. Our company is approximately 70 years old and our network started very small. As the company grew, we maintained the same flat network that included both the data center and the users. When I looked at it, I considered two solutions for separating them. The first was the traditional firewall and a physical LAN, whereas the second approach was using Guardicore. I felt that this was the easier approach..”

Ehud Huminer

CTO at a consumer goods company with 501-1,000 employees

[Read full review](#) 

“We generally used internal firewalls on individual servers with no solution, in terms of overseeing all the firewalls.

In terms of agility, Guardicore Centra is massively easier to control and manage. The security is good. With just the network logs, you get a better view of any active threats rather than in normal firewalls where you may not find out until sometimes after the fact. You can get notified as well..”

Verified user

Infrastructure Analyst/Developer at a university with 1,001-5,000 employees

[Read full review](#) 

“Of the systems that we looked at, Guardicore has the best coverage for legacy operating systems.

We are in cyber defense advice, and we conducted a modest evaluation. We sell both Illumio and Guardicore solutions, but it all depends on the type of customer, the scope, and finally the individual demands of that customer.

We have, I believe, most of our install-based software as Illumio solutions, this is maybe the second install-based for Guardicore.

It all depends on the real consumer, their needs, how the business is structured, and so on..”

Verified user

Senior Security Consultant at a tech consulting company with 1,001-5,000 employees

[Read full review](#) 

“We looked at Illumio and we also looked at Edgewise Networks.

At the time, Illumio was manipulating the built-in firewall of either Windows or Linux. They were essentially just going into the OS and taking over the management of the local firewall, which was good in some regards but it seemed like an older way to do the same thing. Edgewise and Guardicore were more in step in that they actually have an agent that sits between the compute kernel and the networking layer and that manages which sockets are open and how the services are able to talk to one another. That seems like a better and more modern approach. That was one thing in their favor.

We liked a lot of features of both Edgewise and Guardicore. It came down to cost, in the end. We got a better deal with Guardicore. There were a couple of features that I felt meant that Guardicore had more going for it. It seemed like a little bit more of a mature solution at the time. It had been around a little bit longer. It felt like it had some more depth of knowledge and stability, given some of the engineers we spoke with.

Edgewise was very new. Since we talked with them they've actually been acquired by NetScaler. We had a little bit of apprehension in investing in something that might get gobbled up or might fail, because it was a new company. They're both good solutions but we've been happy with the choice that we made..”

Joshua Turner

Manager Network & Security Engineering at Teleflora

[Read full review](#) 

ROI

Real user quotes about their ROI:

“We get an added layer of protection and user analytics that we can give to our directors in the company, so they can be more confident that things are being managed correctly..”

Verified user


[Read full review](#) 

Corporate Operations Manager at University of Strathclyde

“It has saved us a lot of time. We can secure around 500 systems. We are not growing in personnel. So, with our current personnel, I have been able to secure all the systems.

Guardicore Centra has reduced the number of human resources needed to deploy security solutions. We have two people working on segmentation rules as well as some agents taking care of the infrastructure. Before Guardicore Centra, we would have needed at least one more person..”

Jose Luis Guzman

[Read full review](#) 

Cybersecurity Coordinator at MONEX

“I know the ROI is going to be there because I know what the future's going to look like. The only reason we haven't seen as much as we possibly could have is all on us moving slowly. It's not anything to do with Guardicore. I'm really hopeful for the future with them. But right now we've only really secured a handful of applications. That's all gone really well, but we definitely have not realized its full potential. We've got a lot of older applications and it takes time to get people to agree to rebuild the server and put the agent on it.

We're trying to shift all of our servers. Instead of applying it in place, we're actually trying to go through a process of rebuilding all of our servers. During that process we'll move an application from an old server to a new one, put the agent on it, put it in the new network, and then it will be a Guardicore protected area. That's a slow process that we have imposed on ourselves. I see the light at the end of the tunnel. I think it's going to be a great solution but we are far from the end of the road with realizing all the benefits. That's just a result of taking our time and the plan that we created for ourselves..”

Joshua Turner

Manager Network & Security Engineering at Teleflora

[Read full review](#) 

“We do have ROI. First, one client found theft of data that alone justified to the client the cost. They invested heavily, well over a \$100,000 in Guardicore. That was a big purchase with an extensive setup. That discovery led to court cases. Guardicore provided evidence that they required. It was invaluable.

The second, in terms of the ROI, was for clients using Guardicore for the first time. We showed clients what occurs during patch updates, Windows updates, anti-virus updates, etc. Guardicore shows the traffic. You see your anti-virus going through the updates. Some clients they thought they were being attacked until we showed them that these are the patch monitoring servers.

For many years, clients set up updates. They do change control. They set Guardicore up, they check the lock, and they assume its all done. Guardicore shows them that it was done. The clients have proof that their applications will be filtered appropriately.

In terms of the return on investment, it was an invaluable tool to demonstrate that the client's internal practices will be implemented automatically. That blew away a lot of clients the first time they saw it. .”

Fidel Deforte

Solutions Architect at Alturna-Tech

[Read full review](#) 

Use Case

“I am using it for segmentation. If someone has access to a development system, they can't take that development system and access production equipment..”

Verified user

[Read full review](#) 

Information Security Engineering Consultant at a university with 1,001-5,000 employees

“Guardicore Centra is used to ring-fence a crucial, business-critical application.

We completed the AD integration while also attempting to isolate the jump station with an agent..”

Verified user

[Read full review](#) 

Senior Security Consultant at a tech consulting company with 1,001-5,000 employees

“We are trying to centralize our firewalling as well as provide application segmentation and environment segmentation.

We have a couple of aggregators onsite and the rest are on the cloud..”

Verified user

[Read full review](#) 

Infrastructure Analyst/Developer at a university with 1,001-5,000 employees

“We want segmentation for a data center, and we have the problem that we cannot change IP addresses within the data center. So we need a solution. With the Guardicore solution, we can keep the IP addresses.

Additionally, we get agent-based segmentation, and we don't have to change anything on the network. These are the main reasons why we chose Guardicore for micro-segmentation..”

Verified user

[Read full review](#) 

Information Security Consultant at a comms service provider with 11-50 employees

“In our company, we have a data center that has approximately 200 servers running Nutanix. We wanted to protect these servers from both internal and external attacks. By implementing Guardicore Centra, it has given us defense against attacks from the outside, as well as those that originate from inside of the organization.

We protect Microsoft machines, as well as some that are running Linux. We also have an SAP HANA database that is protected by Guardicore..”

Ehud Huminer

[Read full review](#) 

CTO at a consumer goods company with 501-1,000 employees

“In India, one use case is in the banking industry. In general, one customer used it for microsegmentation deployed across four locations.

Another used it for telemetry and microsegmentation. These were deployments for customers in India and the Philippines.

The workloads have been seamlessly integrated for segmentation. The network has been transited smoothly. So, the integration was straightforward and without major issues..”

Uday Varma

Solution Architechtt at Inspira Enterprise

[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.

“Akamai Guardicore Segmentation's deployment is smooth. The deployment team promised us that the implementation would be completed in three weeks, but the product was available within two weeks. .”

Matthias Kropf

[Read full review](#) 

Senior Expert Enterprise Architecture at a manufacturing company with 10,001+ employees

“I would rate my experience with the initial setup an eight out of ten, with ten being easy.

It was pretty straightforward. It didn't take too long to deploy. And it was roughly done within an hour. So implementation isn't overly complex..”

Uday Varma

[Read full review](#) 

Solution Architechth at Inspira Enterprise

“The initial setup is pretty straightforward.

The only thing that matters is that the customers have a strong plan, a good strategy, and a high-level and low-level design. The most exhausting part will be labeling all of your systems. And if the customer in this situation has around 1000 servers, that may be time-consuming..”

Verified user

[Read full review](#) 

Senior Security Consultant at a tech consulting company with 1,001-5,000 employees

“Guardicore Centra's setup was straightforward and I would rate it a seven out of ten. The tool's setup is straightforward as long as you identify the servers and establish the right processes. The tool came with an installation guide and setup took about four to five hours to complete. The deployment depends on the solution size and if the POC is small, the setup is easier and quicker. If you plan for enterprise-wide deployment, then you need to do capacity sizing and planning..”

Verified user

[Read full review](#) 

Specialist Master - Cyber Risk at a consultancy with 10,001+ employees


“I would rate my experience with the initial setup a seven out of ten, where one is difficult and ten is easy to set up.

The technical setup was easy. It becomes more challenging when you start labeling the assets and doing the ring-fencing. You have to go deep into the architecture of the network, the application, and whatever. That’s more difficult, but in the end, it’s easier than doing classic segmentation with a firewall.

The data architecture took one week, but the segmentation logic took months. We are not finished. We started in April, and we are not finished. So, like almost half a year.

We start to define the ring for the ring fences, and then we start with a part of the network with the test environment. We test and then go. The last will be the production. We label the assets, then start a monitoring period to see the data traffic between the assets. Then we go into an alerting phase and finally to a block period..”

Verified user

[Read full review](#) 

Information Security Consultant at a comms service provider with 11-50 employees

“In terms of the initial setup, it is of medium complexity. It's not complex but not simple. You need to understand your network. You cannot do it without understanding what you want and what your strategy is. When you understand the policy and the strategy that you want to implement on the network, it's very easy.

Our implementation strategy was to start with machine learning. Our plan was to run this for one or two days, get it working, and then understand what kind of information they're getting from me and then to continue on from that. The initial deployment will take a maximum of two days.

Implementing segmentation is not difficult but it is more from our side. First, you need to understand the strategy that you want to implement on the network. Then, you need to complete it step-by-step, so that you do not harm anything or block things improperly. You have to give the software time to learn about the connections that you have. Overall, it is very easy to do.

In terms of how long it took us to implement, we have approximately 200 servers and it took a couple of months to implement. This is what I expected because I wanted to take it slowly and make sure that I understand which systems I needed to block, or not..”

Ehud Huminer

[Read full review](#) 

CTO at a consumer goods company with 501-1,000 employees

Customer Service and Support

“We have not contacted technical support, But the Akamai person was extremely well-read on the subject, and there was almost nothing he couldn't answer during the proof of concept project..”

Verified user

Senior Security Consultant at a tech consulting company with 1,001-5,000 employees

[Read full review](#) 

“I did deal with technical support directly. It was good. I was the guy who was calling them. It was never just a call. They tried to understand the problem and the construct and came up with a solution that would assist us. .”

Vishal Chaudhary

Senior Principal Consultant Cloud/DevOps/ML/Kubernetes at Opticca

[Read full review](#) 

“Their support is pretty good. I haven't had to use them that frequently, so I'm not sure about their response times, but when they come and set your stuff up, everything seems pretty good from that end. I would assume the support after that would be similar..”

Verified user

Information Security Engineering Consultant at a university with 1,001-5,000 employees

[Read full review](#) 

“The technical support has been excellent. It is probably one of the best customer services provided by any company. They are helpful, reactive to problems, and constantly work to enable us to do what we want to do..”

Verified user

[Read full review](#) 

Corporate Operations Manager at University of Strathclyde

“It has very robust technical support. We have three or four people with whom we talk on a biweekly or monthly basis. They are very good. They take care of us. If we have any problems with the tools or rules, they are supportive..”

Jose Luis Guzman

[Read full review](#) 

Cybersecurity Coordinator at MONEX

“The response time should be better. Sometimes it’s good, but sometimes it could be better. You have a problem, you need an answer, and then you have to wait. Sometimes they do not talk with an administrator who knows anything about Guardicore. When my colleagues call support, I think my colleagues are experts. And then the support starts with really easy questions. That’s not funny.

So, I want them to be more skilled, like, more educated on the matter..”

Verified user

[Read full review](#) 

Information Security Consultant at a comms service provider with 11-50 employees

Other Advice

“I rate Akamai Guardicore Segmentation an eight out of ten. Adopting the product often involves a greenfield approach, requiring adjustments and careful planning..”

Matthias Kropf

Senior Expert Enterprise Architecture at a manufacturing company with 10,001+ employees

[Read full review](#) 

“I would say that you should use it for micro-segmentation instead of trying to use firewalls. Because some customers try to use other solutions like firewalls, and it's not the best solution.

Overall, I would rate the solution a nine out of ten. It is an amazing solution. .”

KlavsThaarup

Senior Security Consultant at Orange Cyberdefense

[Read full review](#) 

“I would rate the solution a six out of ten. We mostly have enterprise customers for Guardicore Centra. I would advise users to try this out on a handful of servers for the first time (like < 20 servers to begin with). During and after segmentation, monitor the solution for some period to notice how operationally effective it is and the data sources relied upon for building labels, and policies, and ultimately how easy it is to incorporate any changes needed thereafter..”

Verified user

[Read full review](#) 

Specialist Master - Cyber Risk at a consultancy with 10,001+ employees

“Micro-segmentation should be a specific requirement because, nowadays, many built-in solutions offer similar functionality. Akamai provides Guardicore as an external SaaS service for those needing it in a SaaS environment.

However, for on-premises installations, integration with network vendors like Cisco is crucial. This could be done by customers themselves or through partnerships with other network vendors.

Overall, I would rate the solution a seven out of ten. .”

Uday Varma

[Read full review](#) 

Solution Architechct at Inspira Enterprise

“Overall, I would rate the product a seven out of ten. We use Akamai because they have their own enforcement point. This was important for us.

Other micro-segmentation tools use the desktop firewall of Windows or the Linux

iptables firewall, but Guardicore has its own enforcement point and its own agent. This was a key factor. When you start with the implementation, you have to have a clear picture about your labeling. I think it's really important. You have to know what you want to separate from each other. You could go into very deep detail, but the more detail you have, the more complex it becomes. You have to find a balance between detail and complexity. You need the middle way..”

Verified user

Information Security Consultant at a comms service provider with 11-50 employees

[Read full review](#) 

“I feel both companies are trying hard to better themselves, therefore it's difficult to say.

Illumio may be far ahead in six months or the opposite, it all depends on that and the precise moment.

I wouldn't say one product is superior to another; it all depends on the customer's needs and so on. However, in this scenario, the customer has a large number of legacy, old XP, and Windows 2003 legacy servers, as well as other operating systems. In this instance, Guardicore was our recommendation, but for other clients who don't have that history, Illumio is just as excellent as Guardicore.

It's the best, I would rate Guardicore Centra a ten out of ten..”

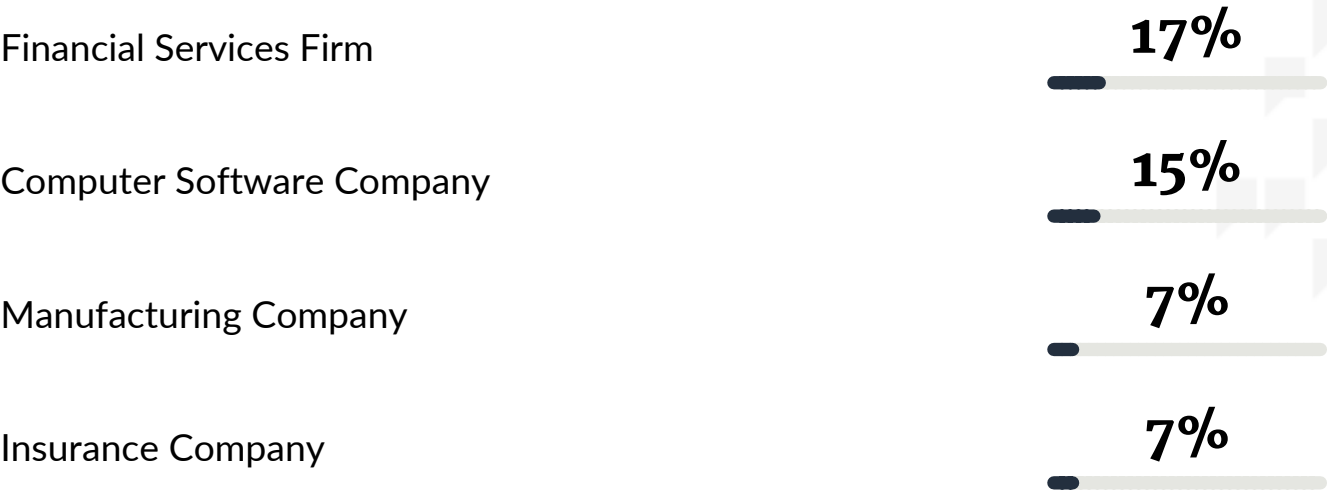
Verified user

Senior Security Consultant at a tech consulting company with 1,001-5,000 employees

[Read full review](#) 

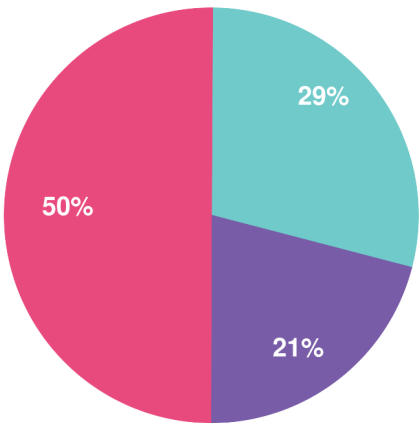
Top Industries

by visitors reading reviews

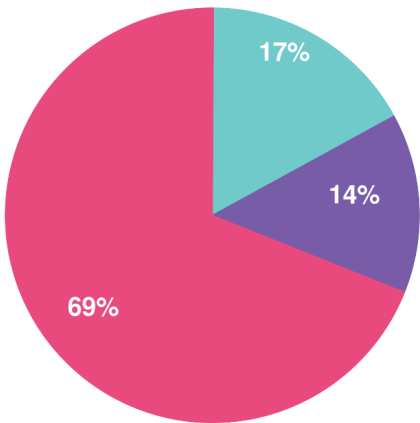


Company Size

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 software running on AWS and other platforms. 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