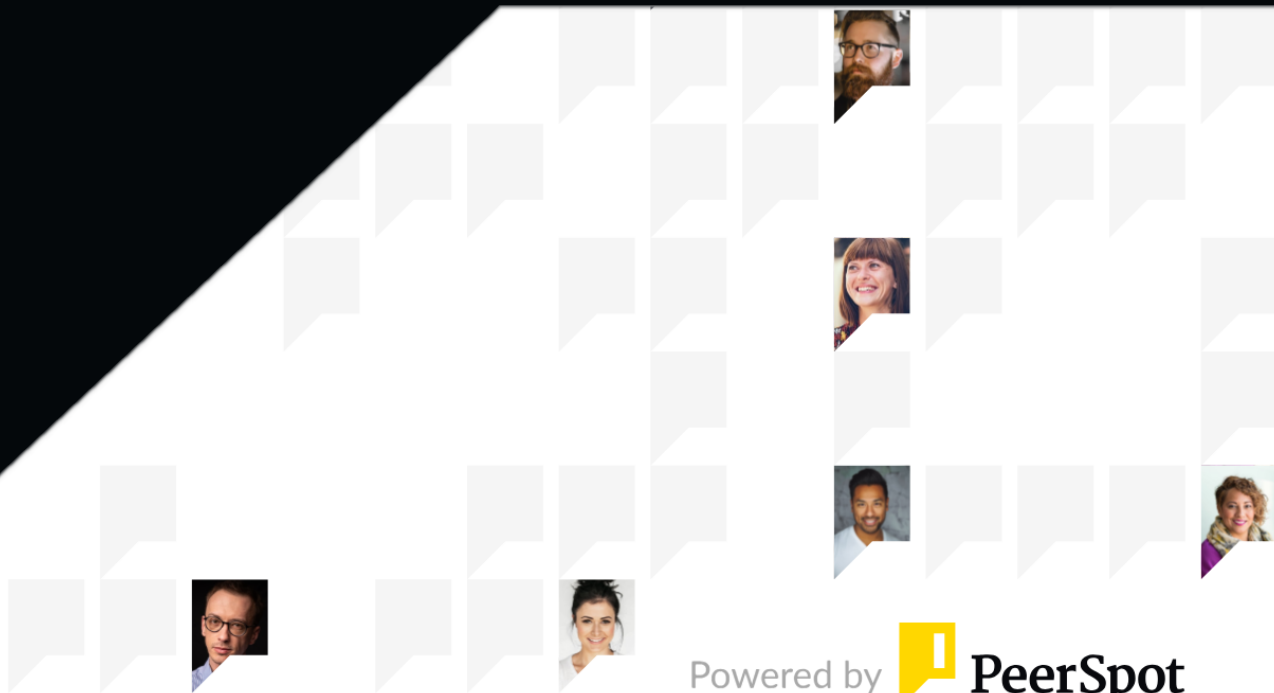


aws marketplace

OPNsense

# Reviews, tips, and advice from real users



Powered by  PeerSpot

# Contents

Product Recap..... 3 - 5

Valuable Features..... 6 - 9

Other Solutions Considered..... 10 - 12

ROI..... 13

Use Case..... 14 - 16

Setup..... 17 - 20

Customer Service and Support..... 21 - 22

Other Advice..... 23 - 26

Trends..... 27 - 28

About PeerSpot..... 29 - 30

# Product Recap



OPNsense

# OPNsense Recap

OPNsense is widely used for firewall functionalities, intrusion detection, VPN and IPSec, content filtering, securing network traffic, and remote access. It protects internal networks and manages servers securely, suitable for small to medium-sized businesses.

OPNsense is a comprehensive firewall solution leveraging open-source technology. It integrates with third-party modules like WireGuard and CrowdSec, enhancing its security capabilities. Offering on-premises and cloud deployment, it features an intuitive graphical interface, advanced reporting, VPN functionality, IDS/IPS features, and high scalability. Users find it ideal for small businesses and home networks due to its stability and ease of use. Frequent updates and an active community support its continuous improvement. However, it needs advancements in VPN selection, scalability, and technical documentation. Enhanced high availability, threat intelligence, and integration with virtualization platforms are required. User feedback suggests improvements in connectivity, alerting, traffic monitoring, and antivirus protection.

## What are the key features of OPNsense?

- Strong Firewall: Robust firewall capabilities for securing network traffic.
- Intrusion Detection and Prevention: Effective IDS/IPS for threat mitigation.
- VPN Functionality: Comprehensive VPN support including WireGuard.
- Content Filtering: DNS-level filtering for enhanced security.
- Advanced Reporting: In-depth traffic analysis and reporting features.
- High Scalability: Supports growing network demands.
- Integration Capabilities: Works with third-party modules like CrowdSec.
- Intuitive GUI: User-friendly graphical interface enhances usability.

## What benefits should users look for in OPNsense reviews?

- Security: High level of protection for internal networks.
- Manageability: Easy management of servers and network traffic.
- Cost-Effective: Open-source nature reduces costs.
- Reliability: Stable performance suitable for small and medium-sized businesses.
- Community Support: Active community and frequent updates.

OPNsense is implemented across various industries to secure network infrastructure and ensure reliable connectivity. In fintech, it safeguards sensitive financial data while maintaining compliance. Educational institutions deploy it to protect student information and enable secure remote learning environments. Healthcare organizations use it to secure patient data and comply with HIPAA regulations. By integrating with tools like WireGuard and CrowdSec, businesses enhance their cybersecurity posture and streamline network management, making

OPNsense a versatile choice for diverse operational needs.

# Valuable Features

Excerpts from real customer reviews on PeerSpot:



“Overall, I would rate OPNsense as nine out of ten.”



**Stephen Zoran**

Senior Client Solutions Architect at a tech services company with 1,001-5,000 employees



“OPNsense is very stable, easy to upgrade, and maintain.”



**Verified user**

Senior Network Engineer at a comms service provider with 11-50 employees



“I mostly rely on the solution's network intrusion detection and prevention system, along with other systems, CMs, and log management.”



**Chiroasca Alecsandru**

Owner at Networks srl



“The DNS-level filtering is impressive for thwarting time scanners.”



**Akram Zaki Hussein**

System and Network Administrator at El Sadat City Language School



“The most valuable feature is the Dual WAN in OPNSense, which offers advanced capabilities.”



**PeterMuiruri**

IT Manager at Pride in Azure



“The solution has high availability.”



**Eddy Ramirez**

IT Security Director at a financial services firm with 1,001-5,000 employees



“It has firewall and VPN capabilities, which are very valuable features.”



**Michael Dietze**

Project Manager at CC GmbH

### What users had to say about valuable features:

The main features I find valuable are ease of use, code stability, and the ability to add features such as Zenarmor, which provides fourth-generation firewall capabilities with deep packet inspection. Additionally, integrating solutions like Tailscale for VPN is very valuable for my uses.

**Stephen Zoran**


Senior Client Solutions Architect at a tech services company with 1,001-5,000 employees

[Read full review](#)

“It is easy to maintain. It is free. So, it is for small offices. It is a very good solution.

I like the dashboard. I can see what is going on and manage it as I like it. .”

**Samo Primožič**

[Read full review](#) 

Technical support engineer at ADVANT računalniški inženiring, komunikacije, svetovanje in distribucija d.o.o.

---

“The DNS-level filtering is impressive for thwarting time scanners. The VPN functionality is also crucial for my needs, as I connect to multiple locations simultaneously. Running the CBN server on the VPN is exceptionally reliable and efficient..”

**Akram Zaki Hussein**

[Read full review](#) 

System and Network Administrator at El Sadat City Language School

---

“The most valuable features include the basic firewall functionality and the GeoIP location services. OPNsense is very stable, easy to upgrade, and maintain. I can work efficiently, knowing it does what it needs to do..”

**Verified user**

[Read full review](#) 

Senior Network Engineer at a comms service provider with 11-50 employees

---



“I mostly rely on the solution's network intrusion detection and prevention system, along with other systems, CMs, and log management. We are currently satisfied with the solution's threat intelligence. It's a pretty much in-house developed solution because it's in a Wazuh server. We have several scripts around it, allowing us to improve our posture on threats..”

**Chirosca Alecsandru**

Owner at Networks srl

[Read full review](#) 

---

“The most valuable feature is the Dual WAN in OPNSense, which offers advanced capabilities. It has cost-effective communication options and the flexibility to deploy on your hardware. I like the security aspects, particularly through package managers. It allows for subscription-based enhancements, providing an additional layer of security to the network..”

**PeterMuiruri**

IT Manager at Pride in Azure

[Read full review](#) 

# Other Solutions Considered

“The configuration and access VPN functionality in OPNsense are satisfactory and work well. Currently, I prefer using Azure Firewall for my firewall needs, even though it might not be the absolute best option. My preference is due to a lack of experience with other Windows-based solutions..”

**Michael Dietze**

Project Manager at CC GmbH

[Read full review](#) 

---

“I have quite a background in Berkeley Software Distribution (BSD) systems. I was looking into BSD, especially for the packet filter side. While evaluating, OPNsense was the most solid solution. I was also considering pfSense as my first option, but it is not so strong on the file system side..”

**Chirosca Alecsandru**

Owner at Networks srl

[Read full review](#) 

“As technical people, we have used many solutions previously for our company and customers. For customers, we have used Fortinet, Palo Alto, and others.

I didn't switch from Palo Alto to OPNsense. I use OPNsense because Palo Alto is used for enterprises. For me, I prefer open-source products. It's more flexible for us..”

**Anwar Sleem**

Regional Director at Ceitcon

[Read full review](#) 

---

“I'm aware of Fortinet as well.

It depends on price versus performance. If you're willing to pay, Fortinet's great. If you don't have the budget, OPNsense is more affordable..”

**Verified user**

Senior Network Engineer at a comms service provider with 11-50 employees

[Read full review](#) 

“I have experience with Check Point and other products like Fortinet. They're different types of tools for different purposes.

My experience is that OPNsense is great for installing and setting up, and then I almost forget about it. It is a good tool for everyday use.

If I require many site-to-site connections or prioritize advanced features, I might look at the other products..”

**Samo Primožič**

Technical support engineer at ADVANT računalniški inženiring, komunikacije, svetovanje in distribucija d.o.o.

[Read full review](#) 

---

“I am currently evaluating and searching for open-source enterprise firewalls and doing a comparison of the features between all of them. I am assessing the pros and cons of vendors.

I am looking for something that will give me a report on the comparison of features, capabilities, the different vendors, and the different open-source solutions that are available.

I am also doing a comparison on Palo Alto, Cisco Firepower, and Fortinet Fortigate..”

**YaserAljohani**

OT/ICS Information Security Specialist at SANS

[Read full review](#) 

# ROI

Real user quotes about their ROI:

“It is now organic, and growing (hope to improve better – though accidents do happen, e.g, COVID, Share market / Financial institution meltdown, the war between nations, and now CyberWarFare picked up!) these are the few key factors which disturb the business one way or other..”

**Raj Ashish**

Founder - Director (Technology Business) at a tech services company with 1-10 employees

[Read full review](#) 

---

“We have witnessed an ROI in less than three months. Money-wise, if I go and look at all the solution that costs money, you're looking at \$5,000 in yearly fees. In this solution, you won't have any recurring fees, and even if you have to pay for equipment and setup, you save that money within three months. .”

**Eddy Ramirez**

IT Security Director at a financial services firm with 1,001-5,000 employees

[Read full review](#) 

# Use Case

“The solution is basically an open-source firewall – a next-generation firewall solution. Now we actually use it at a client or company's request. They use it if they prefer something that is more versatile than a Cisco or Fortinet device..”

**Eddy Ramirez**

IT Security Director at a financial services firm with 1,001-5,000 employees

[Read full review](#) 

---

“I use it for firewall purposes and OpenVPN. Another use is to protect the servers inside my company.

I am using its latest version. It is deployed on my own server..”

**Verified user**

Machine designer at La Poste

[Read full review](#) 

“I use OPNsense primarily for network security. It involves basic firewall operations and GeoIP location functionalities. I've got multiple versions running, some on hardware purchased and some on VPSs..”

**Verified user**[Read full review](#) 

Senior Network Engineer at a comms service provider with 11-50 employees

---

“I moved to OPNsense because it's more secure and more reliable. I use it to secure access to the servers. I have a core backing server, an e-banking server, the main server, and other features with the solution. I make the multi-DMZ packs, so each service is in one DMZ bay, and I use it as a virtual chain..”

**Elisee TAMBA**[Read full review](#) 

Founder/IT Consultant at Open IT World

---

I am a Sales Engineer working for a consulting company. I use OPNsense to take my lab environment on the road for demos. Initially, I built it to bring my demos from my own lab. Although the company has a lab, putting an OPNsense firewall in there worked better because it was a colo. I run it both bare metal and virtualized, and in some cases, I do both.

**Stephen Zoran**[Read full review](#) 

Senior Client Solutions Architect at a tech services company with 1,001-5,000 employees

---

“We started working with a tier-four data center cloud service provider company, and we wish to develop our cloud instance/VM hosted.

We use OPNsense for content filtering, securing networks through DNSs and overcoming the challenges of ransomware, and securing different types of malware-virus attacks.

This is causing a lot of issues because we are focusing more and more on securing our customers' data.

It includes backup, recovery, archival, and now coming up with securing cloud instances/VMs. It is really essential for us.

Example: a firewall as a service can be provided to those who mainly work from home or Soho, Freelancers – clients..”

**Raj Ashish**

Founder - Director (Technology Business) at a tech services company with 1-10 employees

[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 initial setup is straightforward. Being an engineer myself, I have no issues with systems on networks. The installation took around two hours to complete. When you download a system, it takes time. I’ve also installed one package named Zenarmor..”

**Frqncis Massolin**

Cloud Projects Director at France Compétences

[Read full review](#) 

“I would rate the initial setup as seven out of ten because sometimes we are facing issues, particularly with IP addressing. It takes a couple of hours to navigate and make the necessary preparations. Given that OPNsense is open-source, there isn't official support available at the moment, which adds an extra layer of complexity to issue resolution..”

**Akram Zaki Hussein**

System and Network Administrator at El Sadat City Language School

[Read full review](#) 

“The deployment process takes almost an hour. The installation process involves several steps. First, you need to install the software. Then, configure the interfaces as needed. After that, establish the necessary rules for the software to function correctly. Finally, configure the VPN settings to ensure secure communication. I rate the solution a seven out of ten. .”

**Michael Dietze**

Project Manager at CC GmbH

[Read full review](#) 

---

“I believe the setup phase was a fusion of straightforwardness and complexity. It's not complicated, so it's fine.

It's deployed on-premises because we put it on our server, and it is hosted in Germany..”

**Anwar Sleem**


Regional Director at Ceitcon

[Read full review](#) 

“The tool's deployment is easy. Apart from Cisco firewalls and Fortinet, if we talk about Untangle, pfSense, OPNsense, and so on, they are fairly quick to set up. It's not something you spend too much time on. It's a firewall, so you can spend months tweaking the system. If you know what you're doing, you can spend forever on logs, checking and tweaking the system because there's always a new update or feature coming up. Then you start playing with them, tweaking settings, checking logs, blocking or unblocking different things.

You can stay in that loop forever. But for a startup, the initial configuration is fairly easy and quick. It can be completed in 30 minutes. .”

**RicardoDias**

[Read full review](#) 

Network and Programming Specialist at Twentytwo Integration


---

“The initial setup was straightforward for me. It took me approximately two days to set up the system initially. Subsequently, I began testing by progressively increasing the number of connections, deploying it through the unified features, and carefully monitoring specific ports while observing how it handles DHCP releases, IPs, and overall traffic. This process extended over about a week.

To begin the initial setup, you need to search for and download the ISO to initiate the process, followed by a two-step procedure. Afterwards, you proceed with command-line configurations, including setting up IP addresses. Once this initial phase is complete, navigation through the graphical user interface (GUI) becomes more straightforward. However, certain commands and configurations may still pose challenges. I rate it a seven out of ten..”

**PeterMuiruri**

IT Manager at Pride in Azure

[Read full review](#) 

# Customer Service and Support

The support is good. I mainly rely on community support since the solution is open source. I haven't had to open many tickets, just one or two under the Pro license.

**Stephen Zoran**

Senior Client Solutions Architect at a tech services company with 1,001-5,000 employees

[Read full review](#) 

---

“I haven't come across a dedicated support page. I've never had to use it, and generally, with open-source solutions like OPNsense, there's an assumption that there isn't an official support team, unlike proprietary options such as SysTrack, Sophos, or FortiGate..”

**Akram Zaki Hussein**

System and Network Administrator at El Sadat City Language School

[Read full review](#) 

---

“I've only used the free version of the solution. I just have to dig into the forums to find everything I need. There isn't a central place you can reach out to. I've found all the answers I've needed so far via the forums. There's a lot of information there. .”

**Verified user**

Senior Network Engineer at a comms service provider with 11-50 employees

[Read full review](#) 

“The support for OPNsense is good because we have documents available on the internet. The support could improve a little.

I rate the support from OPNsense a four out of five..”

**Amirsaeed Iloukhani**

Security Consultant at Bank Meli Exchange

[Read full review](#) 

---

“To date, we managed to support clients ourselves and whenever we received feedback we come to know that support cost is very high, it is not as local as we are, for small soho, WFH, freelancers, and young startups they prefer locally available partners and hence they are not even interested in talking on those factors..”

**Raj Ashish**

Founder - Director (Technology Business) at a tech services company with 1-10 employees

[Read full review](#) 

---

“I typically use the forum. They don't actually have a contract that you can buy from them for support. Instead, there's a web forum you can reach out to. I know a couple of people on the forum that actually develop the tool, and they are helpful. I've used them only three times over ten years. .”

**Eddy Ramirez**

IT Security Director at a financial services firm with 1,001-5,000 employees

[Read full review](#) 

# Other Advice

Overall, I would rate OPNsense as nine out of ten. The ability to deploy easily and leverage fourth-generation features adds significant value, especially with Zenarmor.

**Stephen Zoran**

Senior Client Solutions Architect at a tech services company with 1,001-5,000 employees

---

[Read full review](#) 

“If you're new to firewalls, I might recommend using this solution. It's very user-friendly, especially for the first-time users.

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

**Samo Primožič**

Technical support engineer at ADVANT računalniški inženiring, komunikacije, svetovanje in distribucija d.o.o.

---

[Read full review](#) 

“It's crucial to have a firewall solution that aligns seamlessly with an open-source approach. Connecting it twice allows for a comprehensive understanding of the network, analyzing factors such as traffic volume, technical specifics, and the nature of inbound and outbound traffic. This step is paramount in selecting the right firewall, considering it provides a holistic view of the network's dynamics. Overall, I would rate it seven out of ten..”

**Akram Zaki Hussein**

System and Network Administrator at El Sadat City Language School

[Read full review](#) 

---

“We do supply the solution and we do use it for ourselves.

I'd advise users to get the Geo functionality. It's a nice add-on, which we make use of a lot. It allows which countries are allowed to access your instances, which is very helpful.

I'd rate the solution at a nine out of ten. .”

**Verified user**

Senior Network Engineer at a comms service provider with 11-50 employees

[Read full review](#) 



“OPNsense is a strong and solid solution that is easy to interact with. I don't see much on the new generation of firewalls, and only a few solutions are available for OPNsense. OPNsense handles network traffic much faster during peak loads because it's on dedicated hardware. I would recommend OPNsense when no specific topic prevents me from recommending OpenSense.

Overall, I rate the solution an eight out of ten..”

**Chirosca Alecsandru**

Owner at Networks srl

[Read full review](#) 

---

“I'm not using OPNsense at the moment. I work with many different technologies and keep testing various setups. Currently, I've gone fully customized. I'm using a Linux server configured as my router and firewall, and I'm using Zenarmor for packet inspection.

This setup allowed me to easily configure SSL VPN and port forwarding for specific ports, which isn't as straightforward with other systems. I've tried several, including Untangle, pfSense, and OPNsense, but found them somewhat restrictive.

OpenSense is quite good. I like it. It has many services and is somewhat similar to the WatchGuard system. I honestly have no complaints; it was a very good experience. It's easy to set up, especially if you know what you're doing. It also offers a nice library of add-ons.

However, if you have appliances with Intel network cards, I would probably go for pfSense instead. Firmware updates and other updates come a bit faster, making it a more reliable service than OPNsense.

Everything that comes up on OPNsense appears first on pfSense. Some features

are not yet available on OPNsense, and they haven't announced a release date. However, I'm confident they will eventually release these features, as they have previously done.

Ultimately, choosing between pfSense and OPNsense is more of a personal preference since they are very similar. Both are FreeBSD systems, operating in similar situations and offering comparable functionality.

Now, I'm just using a Linux server. I can monitor the system, reboot the card, install Apache, and redirect web servers within my home directly to the firewall. This eliminates the need for third-party boxes or other connected computers, allowing me to do everything in the same box. It gives me a lot more freedom.

That's the main reason I stopped using the other systems. I used OPNsense for about six months, which shows I've tried various solutions to find the best one. Despite all the good things I'm saying about OPNsense, I did stay with it longer than pfSense.

I traveled to China, so I used my home as my VPN instead of paying for one. They block VPN services in China, so I was using OpenVPN at home. OpenVPN is a known service, but it gets blocked there. The only way to do it was through SSL VPN, which worked fine. But, talking about OPNsense, everything was working fine. I had no problems. I just had to move away because I needed to use port 443 for something else on my web server, and I can't have a web server together with other stuff. It's a bit more complicated to configure because I use Nginx and Apache, too. You can install these tools on OPNsense, but I found it more complicated than just going onto the command line and doing it.

If you want to use something like OPNsense for FreeBSD, use pfSense instead. Unless, obviously, like me, the person in question has some hardware incompatibility with pfSense. Only then would I go for OPNsense. Because, I mean, they're the same systems, but pfSense is a bit better in terms of overall performance, and security updates come quicker and more often.

I rate the overall product an eight out of ten. .”

**RicardoDias**

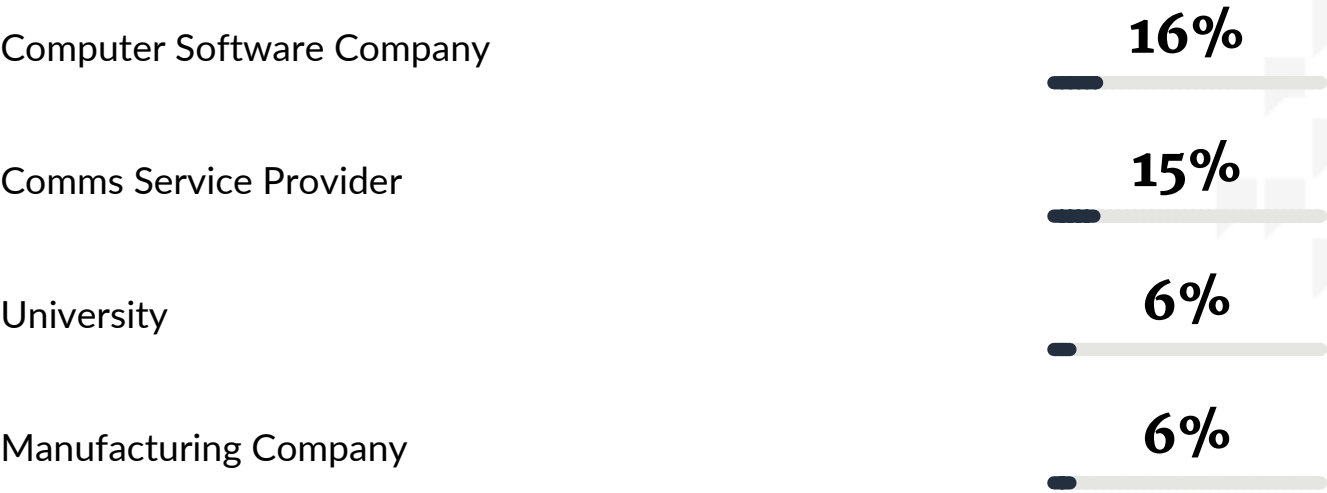
Network and Programming Specialist at Twentytwo Integration

©2025 PeerSpot, All Rights Reserved

[Read full review](#) 

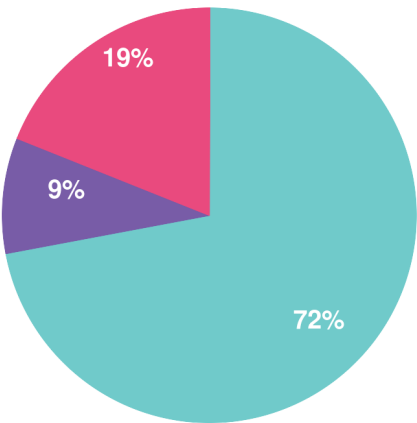
# Top Industries

by visitors reading reviews

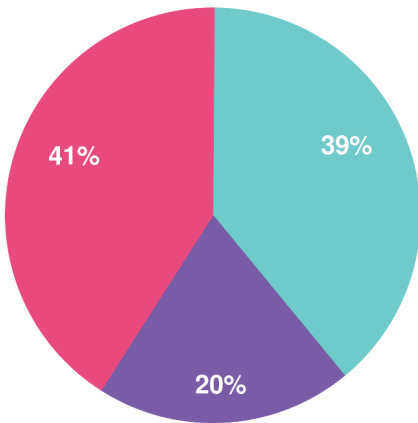


# Company Size

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](http://www.peerspot.com)

## PeerSpot

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

[reports@peerspot.com](mailto:reports@peerspot.com)

+1 646.328.1944