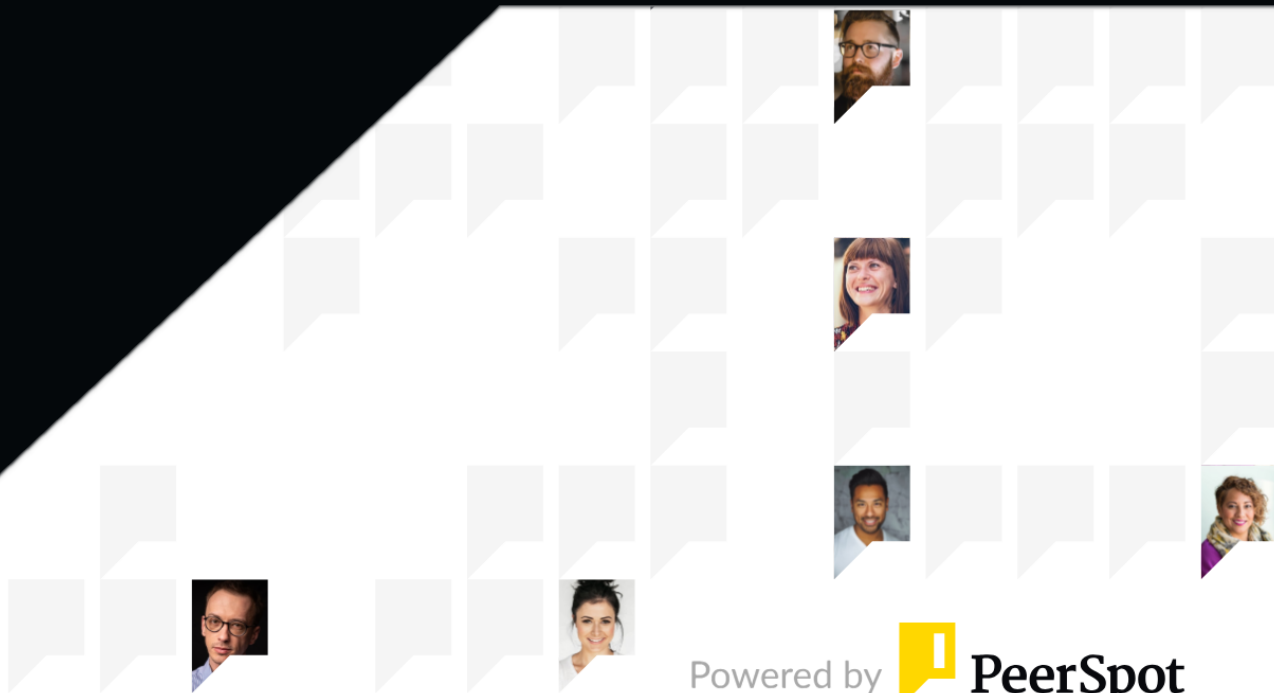


aws marketplace

OPNsense

Reviews, tips, and advice from real users



Powered by  PeerSpot

Contents

Product Recap..... 3 - 4

Valuable Features..... 5 - 12

Other Solutions Considered..... 13 - 16

ROI..... 17 - 18

Use Case..... 19 - 22

Setup..... 23 - 26

Customer Service and Support..... 27 - 29

Other Advice..... 30 - 35

Trends..... 36 - 37

About PeerSpot..... 38 - 39

Product Recap



OPNsense

OPNsense Recap

OPNsense is an adaptable open-source firewall and routing platform appreciated for its flexibility, scalability, and user-friendly interface. It is equipped with robust security features and offers excellent reporting and visibility, essential for small businesses and home setups.

OPNsense stands out for its modular design, allowing cost-effective customization. This system supports VPNs and various firewall capabilities, making it suitable for securing networks from malicious traffic. Its frequent updates and extensive documentation, combined with a supportive online community, enhance user experience. However, there is room for improvement in integration with virtual servers and Azure. Scalability and hardware updates are important for large-scale environments, and users desire more reliable VPN solutions and enhanced threat intelligence tools.

What are OPNsense's most important features?

- **Flexibility:** Easily customizable due to its open-source nature.
- **Robust Security:** Advanced security features for network protection.
- **User-Friendly Interface:** Simplified management and configuration.
- **Frequent Updates:** Regular improvements and new features.
- **Dense Documentation:** Extensive resources and community support.

What benefits should users look for in reviews?

- **Cost-Effectiveness:** Open-source design reduces costs.
- **Scalability:** Ability to grow with business needs.
- **Customizability:** Tailored solutions for different requirements.
- **Community Support:** Access to a strong network of resources and peers.

OPNsense is implemented in industries requiring VPN and firewall functions, supporting site-to-site connections, protecting servers, and managing commercial network traffic. Companies apply it for security, UTM, SD-WAN, content filtering, intrusion detection, and prevention, utilizing its open-source nature and effectiveness as a next-generation firewall.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- ✓ “Based on my experience, the main benefits OPNsense provides for me are due to the limitation in getting financials to implement the most marketable solutions available in the market, which pushed me to find other open-source-related or cheaper solutions, and that is how I came upon OPNsense and pfSense, but OPNsense was the choice in this decision, providing a simple but also effective solution on a low budget.”



Peter Muiruri

IT Manager at a comms service provider with 201-500 employees

- ✓ “For the initial setup of OPNsense, I find that it is very simple.”



ENOCH AMARH ANNOR ATTOH

Cyber Defense Incident Responder at a comms service provider with 11-50 employees

- ✓ “OPNsense impacts my projects and home network positively because its cost-effectiveness is perfect for lab and enterprise setup without expensive licensing, and the flexibility, easy VLAN and DMZ configuration supports different zones such as web servers, mail servers, and log servers.”



Moutaz Sheikh Alard

ISO 27001 Lead Implementer at a consultancy with 11-50 employees



“I find everything valuable in OPNsense; the configuration and reporting aspects are what we require, reporting on user access and data consumed is fascinating in OPNsense, and the configuration offers a clear idea of everything that I have configured in DHCP.”



Dhirender Kumar

IT Executive at M.V.electrosystems



“YouTube provides video explanations, and that brings you to speed, instead of sitting down and reading a 200-page document on the product.”



Harry Fusser

Senior Solutions Engineer at a educational organization with 201-500 employees



“We saved up to half a million Egyptian pounds, which is nearly \$100,000 yearly on licensing or subscription using this kind of software, and the network attacks reduced by approximately 60% after using that, even without customizing the custom configuration yet.”



Mahmoud Suleiman

Senior IT Infrastructure Engineer at a real estate/law firm with 11-50 employees



“OPNsense definitely gives me peace of mind and helps my workflow because of the network isolation, as I can have multiple subnets without having to worry about one affecting the other.”



Richard Chamberlain

Administrator at a retailer with 10,001+ employees

What users had to say about valuable features:

“The functions I find most useful in OPNsense are basically the routes because we have a lot of routing that we do with it, VPN, and specifically WireGuard VPN. We also have the Zenarmor plugin because we do use the Zenarmor plugin, and disk monitoring log, ntop, as we also use it for ntop log monitoring..”

ENOCH AMARH ANNOR ATTOH

Cyber Defense Incident Responder at a comms service provider with 11-50 employees

[Read full review](#)

“YouTube is one of the best features with OPNsense.

“In today's world, it is YouTube that stands out. It is just a big game, with someone writing code, putting it in a box, an embedded system and writing the 200-page manual on how to use it. In my opinion, down the road it is plain old TCP/IP, UDP in terms of communications and it is completely overrated. But this is what we have to live with unfortunately, that is what is out there. YouTube provides video explanations, and that brings you to speed, instead of sitting down and reading a 200-page document on the product..”

Harry Fusser

Senior Solutions Engineer at a educational organization with 201-500 employees

[Read full review](#) 

“In my opinion, the most useful functions or features in OPNsense are those that come packaged inside, such as WireGuard, if you need a VPN. It is not something you have to install afterward. Upon installing OPNsense, you can get WireGuard straight from the interface itself. You can also make it even more advanced by subscribing to certain features to enhance filtering capabilities, especially for filtering websites such as social media and specific traffic types. For pfSense, you cannot get those features straight. You have to keep adding on and installing add-on packages.

Regarding OPNsense's detection capabilities enhancing my network security, it does filter quite a lot. In terms of firewalling, I can really recommend it to someone who does not want to invest much on hardware and software that can really secure their network. As long as you have somebody who understands the product and is also willing to learn, even if they do not know initially, it is something to pursue at a very minimal cost.

When talking about real-time filtering inside the product, I am actually very satisfied with it. It is real-time. I like the way it does it. Upon effecting a rule, it automatically starts working. It is not something that delays or seems to hang the system. It effectively starts working immediately upon deploying the rule..”

Peter Muiruri

IT Manager at a comms service provider with 201-500 employees

[Read full review](#) 

“In my opinion, the best features OPNsense offers are that it's open source, so it can be implemented in whatever scope or environment that I need. I just need to scale the hardware for that environment and I don't have to pay a license, perpetual or renewal.

“The open-source aspect and flexibility of OPNsense have helped me significantly, especially due to the difference in the currency exchange rate here in Egypt, where the licensing and budgeting for IT infrastructure is very hard right now due to the high cost of the products in the Egyptian currency. Most companies see that the IT department is a consuming department, not one that's bringing money, with the ROI being an improvement in SLAs in a few percentages. We have a tight budget in Egyptian pounds, so when we get stuck because the budget has ended, we have to prefer open-source solutions to save budget, and here the open source can rise and shine. I don't need the license, so I will save cost in my budget that I can use in another product that doesn't have any alternative.

“People sometimes overlook that OPNsense is modular, and that you can install plugins to improve it. You don't have to use it bare-metal OPNsense releases; it's modular, and you can add whatever plugin or features that you need to be added..”

Mahmoud Suleiman

Senior IT Infrastructure Engineer at a real estate/law firm with 11-50 employees

[Read full review](#) 

“I find everything valuable in OPNsense. The configuration and reporting aspects are what we require. Reporting on user access and data consumed is fascinating in OPNsense, and the configuration offers a clear idea of everything that I have configured in DHCP.

The key metrics I track to measure the effectiveness of reporting tools include the graphic interface and real-time statistics, which are much better in OPNsense compared to Other products. If I want to export something, that is easy from OPNsense.

“Managing Rules and implenting Policies are much easier than competitive products, Practically using IP blacklisting as well as whitelisting, If we talk about port forwarding, is very straightforward. In OPNsense, everything can be done on a single screen: identifying the source of packets, determining what to do with them, and deciding where they should land is the most convenient aspect.

“Additionally, making group of IP addresses in OPNsense is very easy, making the overall experience very user-friendly.

I assess OPNsense's intrusion detection capabilities through practical testing. I find the load balancing features quite satisfactory as I am using two WANs with this system. The load balancing features have no negative impact on my operations, and I am satisfied with this aspect as it automatically takes over the network, directing load to the second WAN if one fails. .”

Dhirender Kumar

IT Executive at M.V.electrosystems

[Read full review](#) 

“For my capstone, I use OPNsense for my project and its broader benefits for enterprise and cybersecurity context. OPNsense is an open source based firewall and routing platform. It offers enterprise-grade features such as intrusion detection and prevention system, VPN support, traffic shaping, and web filtering, all without license cost. This platform has a modular design, a clean web-based GUI, and frequent updates that prioritize security and usability. It competes with commercial firewalls such as Cisco ASA, FortiGate, and Palo Alto, but stands out because it's community-driven, cost-effective, and transparent.

“I find OPNsense's feature of acting as a central firewall and gateway most valuable, providing robust point segmentation between the internal network and DMZs in my capstone project, intrusion detection to monitor malicious traffic, VPN services for secure remote access, and logging and monitoring for compliance and auditing. This allows me to simulate a real-world enterprise environment on a smaller scale, demonstrating both security hardening and network efficiency.

“OPNsense impacts my projects and home network positively because its cost-effectiveness is perfect for lab and enterprise setup without expensive licensing. The flexibility, easy VLAN and DMZ configuration supports different zones such as web servers, mail servers, and log servers. The security-first design for IDS/IPS integration helps me showcase modern defense-in-depth strategies. The user-friendly management through the web GUI makes it possible to manage complex firewall rules clearly, which is critical when documenting and presenting a capstone. Scalability is also an advantage. Although my project is lab-based, OPNsense can scale into production deployments in SMBs and enterprise..”

Moutaz Sheikh Alard

ISO 27001 Lead Implementer at a consultancy with 11-50 employees

[Read full review](#) 

Other Solutions Considered

“Before choosing OPNsense, I evaluated pfSense, but pfSense is maintained by Netgate, which has filed for bankruptcy, so it's considered legacy and not fit for the modern network. OPNsense is a good option..”

Mahmoud Suleiman

Senior IT Infrastructure Engineer at a real estate/law firm with 11-50 employees

[Read full review](#) 

“I have been working with firewall solutions for about two years. I first worked with pfSense, then I was looking for a difference. That is when I came across OPNsense and wanted to know the difference between the two of them and how OPNsense might be better than pfSense, and also the vice versa..”

Peter Muiruri

IT Manager at a comms service provider with 201-500 employees

[Read full review](#) 

“In my opinion, the main competitors for OPNsense in the market are Arista and Ubuntu, especially Untangle from our end. I prefer Untangle. Because I am using more of OPNsense, I will be partial here..”

ENOCH AMARH ANNOR ATTOH

[Read full review](#) 

Cyber Defense Incident Responder at a comms service provider with 11-50 employees

“When it comes to comparing OPNsense with other vendors, I cannot compare because currently OPNsense is fully open source. Compared to other vendors who claim to be open source but somehow they still have some interference with their product, yet they claim to be open source, OPNsense stands apart. I can only compare OPNsense with pfSense, since those are the only two I have worked with. pfSense currently, even the community, is not fully open..”

Peter Muiruri

[Read full review](#) 

IT Manager at a comms service provider with 201-500 employees

“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 selected OPNsense as a primary solution in my project because of its strong open-source community support, robust features, and suitability for a cost-effective lab environment. If I were to switch to another solution, the most likely candidate would be pfSense or a commercial firewall appliance such as Cisco ASA or FortiGate.

“For pfSense, built on a similar FreeBSD foundation with a long-standing reputation in academic and enterprise labs, I might choose it if I need certain community plugins or enterprise-level add-ons that are more mature in pfSense. The reason I initially didn't switch away from OPNsense is that it provides everything required for my capstone: VLANs, DMZ segmentation, IDS/IPS integration, VPN functionality, logging and monitoring, strong documentation, and GUI management. But for a production environment, I might recommend switching to Cisco or FortiGate for scalability in a very large network to ensure professional support in case of critical downtime and integration with another enterprise security system.

“Before choosing OPNsense, I evaluated other options to ensure the choice aligns with both the technical goals of my project and real-world industry practice. The main alternative I considered was pfSense, which is very close to OPNsense. Both are free-based. I considered it because it's widely used in academic labs and has a strong plugin ecosystem. Ultimately, I preferred OPNsense for its more modern user interface, frequent updates, and strong focus on security features..”

Moutaz Sheikh Alard

[Read full review](#) 

ISO 27001 Lead Implementer at a consultancy with 11-50 employees

ROI

Real user quotes about their ROI:

“Unfortunately, I have not seen a return on investment with OPNsense; I don't keep track of that, beyond the sense of saying that for a very little investment, I was able to increase the security of my network..”

Richard Chamberlain

Administrator at a retailer with 10,001+ employees

[Read full review](#) 

“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

[Read full review](#) 

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

“I have seen a return on investment as I saved a chunk of money, nearly \$100,000, needed for licensing for an enterprise firewall such as FortiGate or Sophos.

“We saved up to half a million Egyptian pounds, which is nearly \$100,000 yearly on licensing or subscription using this kind of software. This saved a huge amount of money, and the network attacks reduced by approximately 60% after using that, even without customizing the custom configuration yet. Currently, I'm working on custom configuration..”

Mahmoud Suleiman

[Read full review](#) 

Senior IT Infrastructure Engineer at a real estate/law firm with 11-50 employees

Use Case

“I mainly use OPNsense for routing and network security. That is the basic use: routing and firewall, basically for connecting to the internet as well as filtering my outgoing and incoming traffic..”

Peter Muiruri

IT Manager at a comms service provider with 201-500 employees

[Read full review](#) 

“I work with OPNsense to create my capstone project in the sixth semester. I work with OPNsense for my capstone project, and I am now planning to make it my main firewall in my network at home, and I'm planning to use it also in case I work in the company..”

Moutaz Sheikh Alard

ISO 27001 Lead Implementer at a consultancy with 11-50 employees

[Read full review](#) 

“I am using OPNSense at 5~6 Different Locations with different network requirements, having 40-80 clients each and fully depend on OPNSense and it is running satisfactorily. After running OPNSense for 5 years at my primary location management has engaged another firewall solution. Now my primary setup is shrink to 7 to 8 computers which is playground for me and my colleagues. But we are successfully handling OPNSense at other locations remotely . .”

Dhirender Kumar

IT Executive at M.V.electrosystems

[Read full review](#) 

“My main use case for OPNSense is that it is my home firewall for my home lab.

“A quick specific example of how I use OPNSense in my home lab is that I use VLANs, so I have different networks or sub-networks inside my home network, and the VLAN inside of OPNSense allows me to keep them isolated.

“I have added some firewall rules to allow different devices to talk to different subnets regarding how I'm using OPNSense in my home lab..”

Richard Chamberlain

Administrator at a retailer with 10,001+ employees

[Read full review](#) 

“We work on the technological side of things, systems, automation systems. When it comes to Layer 2, 3, 4, we hit firewalls. We work with a big company in the United States, so we usually use their recommended ones. There is a certain flexibility for products. We are not bound to buy a certain product, so it is flexible.

“This is not robotics; that is process automation. It involves DCSs, PLCs, that type of systems.

“DCS refers to control systems and PLCs (Programmable Logic Controllers). It is basically automation for processes such as refineries, chemical factories, paper mills, so that is what we do.

“We have been using OPNsense in a lab, so we are actually experimenting with it..”

Harry Fusser

Senior Solutions Engineer at a educational organization with 201-500 employees

[Read full review](#) 

“My main use case for OPNsense is as a firewall on-premises.

“Using OPNsense in my work environment, it serves as the first line of defense. I'm using it for filtering, using my own repository and Dnsmasq to filter unwanted websites. I'm using it as an SD-WAN, as an IPS, intrusion prevention software, and as a next-gen firewall.

“As the first line of defense of my network, OPNsense firewall acts effectively, helping me reduce the number of attacks that my network suffers or has been impacted by a huge percentage. Due to its openness and because it's free, and it's a next-gen firewall, it can go up to the application layer to protect my network, which is very good and unique compared to traditional firewalls.

“OPNsense is deployed on-premises in my organization..”

Mahmoud Suleiman

Senior IT Infrastructure Engineer at a real estate/law firm with 11-50 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.

“Regarding the initial setup for OPNsense, I find it fair and not that complex. As long as you have knowledge of Linux, it is simple and very straightforward..”

Peter Muiruri

[Read full review](#) 

IT Manager at a comms service provider with 201-500 employees

“I do not think there is a difference. All these products that are out there are more or less on the same level when it comes to setting up OPNsense initially..”

Harry Fusser

[Read full review](#) 

Senior Solutions Engineer at a educational organization with 201-500 employees

“Regarding the pricing, OPNsense has no cost. The setup is somewhat easy, and for licensing, I haven't tried the paid version yet, but overall it's perfect. I save time while working on my capstone project because OPNsense helps me save time during setup and configuration, especially for the intrusion prevention system that helps me be more aware of monitoring and catching any malicious packets or traffic already passing through my network..”

Moutaz Sheikh Alard

[Read full review](#) 

ISO 27001 Lead Implementer at a consultancy with 11-50 employees

“My experience with pricing, setup cost, and licensing for OPNsense has been very positive since it is open source, reducing the cost of licensing. I don't need to license the software as it's free, and I can also scale the hardware, which cost me around 30,000 Egyptian pounds, less than a thousand dollars for used servers. This initial cost just required purchasing the server and installing the open-source software, reducing the amount of money needed for an enterprise firewall..”

Mahmoud Suleiman

[Read full review](#) 

Senior IT Infrastructure Engineer at a real estate/law firm with 11-50 employees

“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

[Read full review](#) 

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

“For technical support, since I have not worked with one that requires external support, in my case, I think I can give it a ten, because I am able to manipulate whatever I want, and whatever I want it to do, it does. It does not disappoint. So for me, technically, it is a ten..”

Peter Muiruri

[Read full review](#) 

IT Manager at a comms service provider with 201-500 employees

“My mark for OPNsense technical support is a four for the free version since they do not care when they realize you are using the free version; they just ghost on you. For the paid version, I give them a seven or eight because once you are paying, they want to pay attention to you, but if it is free, they do not care and just ghost on you..”

ENOCH AMARH ANNOR ATTOH

[Read full review](#) 

Cyber Defense Incident Responder at a comms service provider with 11-50 employees

“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](#) 

“In my personal experience, I mostly interact with the community side and find it responsive and well documented. The forums answer most configuration issues I face, and the documentation is up to date. Compared to some open-source projects with weak support, OPNsense stands out for having both a strong community and commercial backing options..”

Moutaz Sheikh Alard

ISO 27001 Lead Implementer at a consultancy with 11-50 employees

[Read full review](#) 

“I have not had that chance yet with OPNsense, but this might be a good point. This is a differentiator. It is not just OPNsense firewalls, it is any other gizmo provider out there. You have Dell, you have Microsoft. Try to get support. The first question they ask you is about your support contract. If you say you do not have one, it is finished. This is where the monopoly starts. I am not sure how it is with OPNsense. If you call for support, it would be a test, actually. I have not done that yet. They might let you hang, saying you need a support contract, and finish. I do not know..”

Harry Fusser

Senior Solutions Engineer at a educational organization with 201-500 employees

[Read full review](#) 

Other Advice

“I rate OPNsense 8 out of 10. It is a straightforward product that has nothing crazy to do with it.

“My advice for others looking into using OPNsense is to get creative.

“My company does not have a business relationship with this vendor, as we are just customers..”

Mahmoud Suleiman

Senior IT Infrastructure Engineer at a real estate/law firm with 11-50 employees

[Read full review](#) 

“Regarding intrusion detection capabilities for network security, I think it is fine.

“When it comes to the load balancing feature in OPNsense, I have seen it, but I have not used it. What I have actually been trying to use is the high availability—that is the groupings.

“I cannot rate the pricing for OPNsense. I would rate this product an overall eight out of ten..”

ENOCH AMARH ANNOR ATTOH

Cyber Defense Incident Responder at a comms service provider with 11-50 employees

[Read full review](#) 

“The advice I would give to others looking into using OPNsense is to absolutely go play with it. For little cost, if you have an extra machine around that you can test it

out on, test it out. I'm running it on a low-end mini PC with multiple network interfaces and it works great.

“I would say that OPNsense is one of those technologies, a firewall that if you're not playing with, you should, just to keep your skills up and to secure your home network.

“On a scale of 1–10, I rate OPNsense an 8..”

Richard Chamberlain

Administrator at a retailer with 10,001+ employees

[Read full review](#) 

“The GUI-based OPNsense is very useful and easy to deal with because many people find it frustrating to deal with command line projects. OPNsense provides a web-based GUI that makes the matter easier and more efficient to look at and to deal with.

“I will discuss the general benefits of OPNsense, which include compliance support that is useful for organizations pursuing ISO 27001 and PCI DSS, as it helps enforce security controls. One benefit is open-source transparency; unlike black-box firewalls, its code is reviewable and trusted by the community. Rapid innovation through frequent updates means it stays aligned with modern threats, and many organizations use OPNsense as a cost-effective alternative to commercial appliances without sacrificing core security capabilities.

“From using OPNsense, I think it could be easier, and I will talk about the lessons I learned. I gained hands-on experience with firewall rules design and the challenges of balancing security with usability. I learned the importance of logging and monitoring for incident response. Furthermore, I realized that open-source tools such as OPNsense can be viable for both learning and professional deployment. Most importantly, OPNsense helped me connect academic theory with practical enterprise-grade solutions.

“I rate OPNsense a nine because the documentation needs more clarification.

“If I were advising others considering OPNsense, I recommend a few key points. Start with clear goals; OPNsense has a wide feature set including firewalling, IDS/IPS, VPNs, traffic shaping, and more. Define what you need first—segmentation, remote access, monitoring—so you don't get overwhelmed. Invest in proper hardware since performance and scalability depend heavily on CPUs, RAM, and network interfaces, especially for IDS/IPS. Choose hardware with enough power; otherwise, packet inspection can slow the network. Leverage the community by utilizing the forums, [GitHub](#), and documentation, which are excellent. Most configuration challenges I face have already been solved by others. Keep it updated because OPNsense has frequent updates and security patches. Staying current ensures you are protected against new vulnerabilities. For labs and mid-sized enterprises, open source is a fantastic solution; it is cost-effective, feature-rich, and transparent. For very large enterprises that require vendor SLAs or guaranteed throughput, you may want to evaluate commercial appliances alongside OPNsense..”

Moutaz Sheikh Alard

ISO 27001 Lead Implementer at a consultancy with 11-50 employees

[Read full review](#) 

“We would have to do testing with OPNsense in an environment doing pen tests using cybersecurity tools that are available to pen test and see what happens. Because I am not in the IT group, and this is not our focus anyway, we have not done this bench testing, benchmarking, firewalls, or whatsoever, on-premises or not, all versions, hardware related, software firewalls.

“With OPNsense, I find that you have to actually worry about this. There are two opinions on this. If I were an IT person, I would say it is fine, but I am not. I am an engineer. When I look at this IT stuff, in my opinion, this is in today's world completely overrated for what it is supposed to do. The fact that it is public makes it just not safe. And the rest is just a game. Firewall A, B, C, D, E, F, G, standard 1, 2,

3, 4, 5, 6, 7, 8. It will never be safe as long as it is public.

“You want a game changer, you have to make the networks private. And this has to run not through your little company, it has to run through the ISP. It is the internet community that has to handle this. I cannot predict it, but this public stuff over there is public. In the end, whatever is public-facing is not safe. I make sure I have backups in place. When something crashes, I restore as quick as I can.

“I do not use OPNsense VPN features.

“As a company, this is a big game that is being played. I do not appreciate this because I am actually a chemical engineer and I want to focus my energy on how to make products with better quality, more efficient, using less energy, less raw materials, and so forth. [Here](#) you are stuck with running a game just to get simple communications up safely because it is on the public internet, which makes absolutely no sense. Instead of being a boon for remoting and productivity enhancement, I think we have reached the point where it is the opposite.

“There are many ways down the road I see that will happen, probably some private type of networks that businesses get from the ISPs, private connectivity, so that you can clearly separate what is public and what is not. All you see happening and this patching up is IP version 4, NATting, PATting, it makes no sense. We try to keep things isolated as much as we can. Whenever it comes to a business-related solution, we will always go with a provider. We are actually outsourcing it; we are not doing it ourselves.

“My rating for OPNsense is 5 out of 10..”

Harry Fusser

Senior Solutions Engineer at a educational organization with 201-500 employees

[Read full review](#) 

“I confirm that I am currently still working with OPNsense and still using their product. However, because of the hardware that I am using, sometimes it ends up

freezing quite often, especially the interfaces, most of the busy interfaces. This is because I am not using the recommended network interfaces for that matter, as I have customized a normal desktop computer to work as an OPNsense router. Because of using the TP-Link cards, that is why I am getting frustrated. I was planning to find, either from the community, the best specification of a computer, maybe an old computer that one can use. Or, because I do not want to invest much on the hardware, I will buy network-dedicated cards, like the Intel cards, since it is not the CPU that has a problem.

In terms of OPNsense's VPN functions, I normally use it to access it from outside the workplace or to have some of the roaming users access the premise resources from outside the premise. Though, I was also looking at the SD-WAN capability of OPNsense because I wanted to find out if it is possible to have an SD-WAN solution with OPNsense. We are a business that has eight different branches, so I was looking for a way I can have each branch with an OPNsense, but then interconnect all of them through an SD-WAN solution instead of IPsec. This is so that you can communicate with the data center where we have hosted our servers, through OPNsense. I was looking for that to be one of the options: either use IPsec or use a public LAN such as Tailgate.

In terms of the reporting tools for my network traffic analysis, the reports are good. OPNsense has good reports in terms of the basics: the DHCP, the IPs already given out. In terms of whatever is blocked, whatever has been detected to be a potential threat, and the source of these threats, from which particular region, you can easily get the report from there. Also the bandwidth utilization, you can get it from there. I also deployed it some time back and I saw it had the capability, which of late I cannot see, to incorporate it with a wireless management system such as the Unifi.

Regarding the load balancing features in OPNsense, I have also used it in terms of load balancing and failover. It is also very effective and straightforward. You just need to have the knowledge on how to go about it. Since it is a community-based open source, you can easily get the information online in case of anything. I have tried both load balancing and failover and it has worked very effectively. In terms

of quality of service also, it is very effective. I cannot complain.

Based on my experience, the main benefits OPNsense provides for me are due to the limitation in getting financials to implement the most marketable solutions available in the market. That pushed me to find other open-source-related solutions or cheaper solutions. That is how I came upon OPNsense and pfSense, but OPNsense was the choice in this decision. That is what brought me to finding a simple but also effective solution, but at a low budget.

I did not purchase OPNsense directly from the vendor or through marketplaces. I just downloaded the ISO file from OPNsense. In terms of price, I think OPNsense has a reasonable price compared to others, so I can give it about an eight or nine. I would rate this review as a nine overall..”

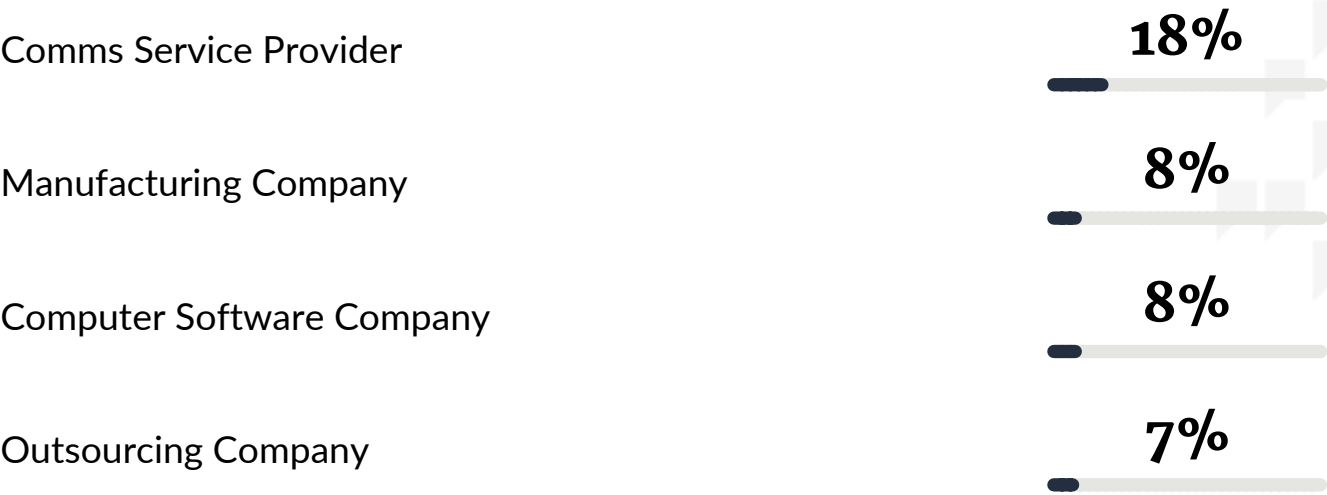
Peter Muiruri

IT Manager at a comms service provider with 201-500 employees

[Read full review](#) 

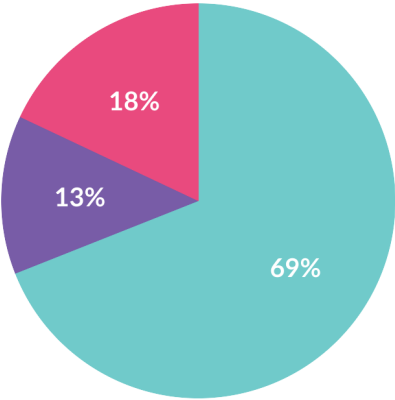
Top Industries

by visitors reading reviews

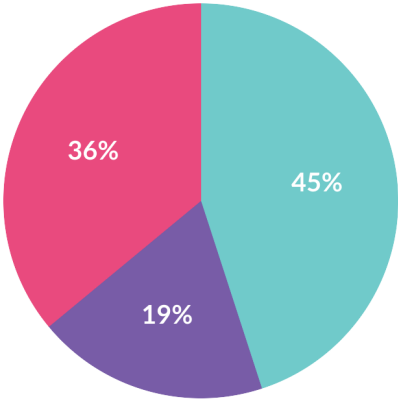


Company Size

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