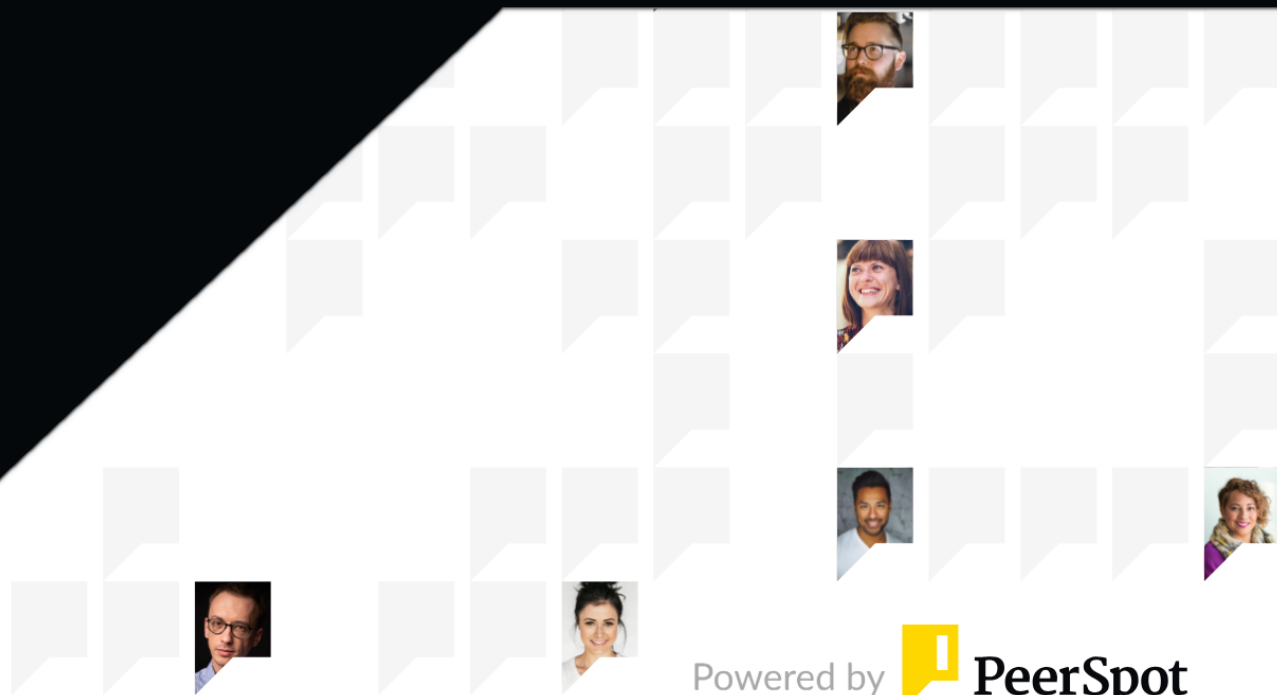




Security Onion

Reviews, tips, and advice from real users



Powered by  **PeerSpot**

Contents

Product Recap..... 3 - 4

Valuable Features..... 5 - 11

Other Solutions Considered..... 12 - 13

ROI..... 14 - 15

Use Case..... 16 - 19

Setup..... 20 - 22

Customer Service and Support..... 23

Other Advice..... 24 - 28

Trends..... 29 - 30

About PeerSpot..... 31 - 32

Product Recap



Security Onion

Security Onion Recap

Security Onion is an open-source Linux distribution for intrusion detection, network security monitoring, and log management. It offers comprehensive solutions for enterprises seeking to enhance their cybersecurity infrastructure.

Security Onion provides a full suite of tools to detect and respond to cybersecurity threats efficiently. As a robust and versatile distribution, it includes capabilities for real-time analysis, network visibility, and threat detection, making it indispensable for security operations centers. Users value this tool for its integration of open-source software with advanced analytics, affording professionals a detailed overview of network traffic and potential intrusions.

What are Security Onion's most important features?

- **Intrusion Detection:** Utilizes Suricata or Zeek for effective threat monitoring.
- **Network Security Monitoring:** Offers powerful visualization tools for network analysis.
- **Log Management:** Centralizes log collection and analysis.
- **Comprehensive Dashboards:** Provides integrated dashboards for threat visibility.

What benefits or ROI should you look for in reviews?

- **Cost Efficiency:** Reduced cybersecurity costs due to its open-source nature.
- **Improved Threat Detection:** Enhanced ability to identify and respond to threats quickly.
- **Integration Capability:** Seamless integration with existing security infrastructures.
- **Scalability:** Support for scaling network security operations as needed.

Security Onion finds extensive application in industries such as finance, healthcare, and government sectors, where robust network monitoring is critical. Its ability to integrate with existing security tools makes it a preferred choice for organizations looking to strengthen their cybersecurity posture.

Valuable Features

Excerpts from real customer reviews on PeerSpot:



“Security Onion is reliable and is a good product, having no glitches or latency problems.”



Bhanwar Lal

Network Engineer at Crisp System India Pvt Ltd



“What I appreciate most about Security Onion is that it combines multiple security monitoring tools into one platform.”



Matthew Sexton

Help Desk



“Security Onion has positively impacted my organization by enabling students to analyze logs, understand network traffic, comprehend intrusion detection, and utilize threat hunting and incident response skills in a practical environment, which are best practices we have implemented with the students.”



Hamidreza Talebi

BCGEU Faculty, Computer Information Systems Administration at a educational organization with 1,001-5,000 employees

- ✓ “Security Onion brings these tools together in one platform, making it easier to investigate security events and understand what's happening across the network.”



Edward Okereke

Cybersecurity Practitioner at Social Leader

- ✓ “Security Onion is a completely open-source and free platform, making it a cost-effective solution that works smoothly and effectively for our organization.”



Hiten Nandasana

Angular developer at Flourish software

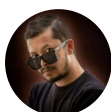
- ✓ “Security Onion is the most mature solution in the market.”



Jörg Kippe

Scientist at a educational organization with 10,001+ employees

- ✓ “The most valuable feature of Security Onion for security monitoring is its ability to find infected ports.”



Anish Bajracharya

Postgraduate at a educational organization with 1,001-5,000 employees

What users had to say about valuable features:

“We are only working with open-source products. The tool is very easy to install and easy to update. A lot of interfaces are specified. So, it's quite easy to make extensions. It is very important when we do experiments and try to connect and integrate other tools. Security Onion is the most mature solution in the open source world. This is its biggest advantage..”

Jörg Kippe

Scientist at a educational organization with 10,001+ employees

[Read full review](#) 

“The most valuable features of Security Onion are its threat detection capabilities, centralized log management system, and network security monitoring.

“Security Onion has positively impacted our organization by providing features such as log management and threat detection, alongside network security monitoring, which creates a significant impact in our environment, particularly in incident investigation support..”

Hiten Nandasana

Angular developer at Flourish software

[Read full review](#) 

“What I appreciate most about Security Onion is that it combines multiple security monitoring tools into one platform. Rather than having to install and manage Zeek, Suricata, and other tools separately, I can work with them in a centralized environment. I also appreciate that it is free and open-source, making it accessible for people building cybersecurity labs.

“Having everything in one place with Security Onion has definitely saved me time because it is one install and then everything is there, so I can learn everything all at once without having to have multiple things running at one time..”

Matthew Sexton

Help Desk

[Read full review](#) 

“One of the best features that Security Onion offers is that it is open source, free to install in a lab environment, and allows for monitoring network traffic and investigating potential attacks while integrating other tools such as Suricata, Zeek, and Elastic-based components that are useful for diving into the logs, along with its threat detection capabilities to see network activity, including port scans, unusual connections, and potential intrusion attempts.

Security Onion's threat detection feature is very useful, and its dashboard is also impressive, showing graphs and allowing me to set alerts to my email or search based on events.

The governance and security of Security Onion are good in terms of how I can investigate through logs and match them with various frameworks, benefiting from being open source when working with enterprise-level organizations.

The accuracy and reliability of output from Security Onion, which is a feature recently added, will be useful for detecting alerts and minimizing false positives during investigations..”

Hamidreza Talebi

BCGEU Faculty, Computer Information Systems Administration at a educational organization with 1,001-5,000 employees

[Read full review](#) 

“The biggest advantage I found when using Security Onion was that it has a combined set of tools, which is beneficial, as having one place with multiple tools is advantageous.

“I have used Elastic Stack for data visualization, last using it maybe a couple of months back. Elastic Stack was helpful for my security operations as it is an open-source tool, allowing me to use multiple tools in one place instead of using them all separately.

“I have also tried Zeek, but I do not use it multiple times. I did not have enough time to understand if Zeek was effective or not, and I did not see much benefit from it.

“I find the intrusion detection capabilities of Suricata beneficial. With Suricata, we can write different rules for different signatures, which allows for customized use cases. It was helpful to aggregate all the events and traffic in one place with Security Onion, so it is beneficial..”

Bhanwar Lal

Network Engineer at Crisp System India Pvt Ltd

[Read full review](#) 

“Security Onion offers a lot of good features. The best feature for me is how it brings different security monitoring tools together in one platform. I particularly appreciate Suricata for detecting suspicious activity, Zeek for analyzing network connections, and Elastic Hunt for investigating alerts and searching logs. Another feature I really appreciate is packet capture analysis because it allows me to examine network traffic more closely and understand what actually happened. I also appreciate how I can move from an alert to related logs and investigate the source and destination IP address, the port, and timestamp. Overall, what makes Security Onion valuable to me is that it gives me different ways to investigate an incident without constantly switching between separate tools. It makes threat detection, troubleshooting, and security investigation much easier.

“Packet capture is one of the features I find most useful in Security Onion because it gives me a deeper understanding of what's happening on the network. For example, when I investigate a suspicious connection, I usually start with the Suricata alert, then check the Zeek logs for the source and destination IP address, port, and timestamps. From there, I can examine the packet capture using tools such as Wireshark to understand the actual traffic behind the alert. It helps me to determine whether the activity is genuinely suspicious or just normal network behavior. It also provides additional evidence that may not be obvious from the alerts alone. Packet capture helps me to investigate incidents faster and make better decisions because I'm not relying on just one alert..”

Edward Okereke

Cybersecurity Practitioner at Social Leader

[Read full review](#) 

Other Solutions Considered

“We also use Malcolm. It is a similar platform. But it is not as mature as Security Onion. The system management features are not perfect and need to be improved..”

Jörg Kippe

Scientist at a educational organization with 10,001+ employees

[Read full review](#) 

“Security Onion is the first easily available, open-source tool with multiple tools in one place, which is why I chose it. For simulation, I use Ixia, which is a similar product to Security Onion..”

Bhanwar Lal

Network Engineer at Crisp System India Pvt Ltd

[Read full review](#) 

“I have considered other products such as Splunk, FORTISiem, and QRadar while I used to work with QRadar, and I find Splunk to be a strong competitor due to its straightforward installation and very graphical user interface..”

Hamidreza Talebi

BCGEU Faculty, Computer Information Systems Administration at a educational organization with 1,001-5,000 employees

[Read full review](#) 

“I did not evaluate other options before choosing Security Onion because I thought it would be the best one to learn, as it has everything built into it and can be used as a standalone..”

Matthew Sexton

Help Desk

[Read full review](#) 

“Before using Security Onion, I worked with tools such as Wireshark and TCP dump to capture and analyze network traffic. Those tools were useful, but I had to investigate the information manually, which took more time. I moved to Security Onion because it brings several security tools together, including Suricata, Zeek, and Elastic. Instead of just looking at network packets, I can also review alerts, search logs, and correlate suspicious activity. The biggest reason I switched was to have a more complete security monitoring environment and make my investigations faster and more organized..”

Edward Okereke

Cybersecurity Practitioner at Social Leader

[Read full review](#) 

ROI

Real user quotes about their ROI:

“We achieve a return on investment through improved threat detection and faster incident response in log management and centralized visibility across the infrastructure..”

Hiten Nandasana

Angular developer at Flourish software

[Read full review](#) 

“With this kind of tool, students can save money by using open-source software while gaining experience in working with different logs and detection systems, leading to time savings during their studies..”

Hamidreza Talebi

BCGEU Faculty, Computer Information Systems Administration at a educational organization with 1,001-5,000 employees

[Read full review](#) 

“I do not have any relevant metrics to share regarding return on investment, but I believe it has saved me time and since it is free, it has not cost me any money. I view it as a good learning tool..”

Matthew Sexton

Help Desk

[Read full review](#) 

“I have seen a positive return on investment for my projects, mainly in time-saving and access to security tools without additional license costs. For example, when investigating a network scan or suspicious login activity, I can review Suricata alerts, Zeek logs, and packet captures in one investigation workflow instead of checking everything separately. This has made my investigation faster and more organized. Since I use Security Onion for independent cybersecurity projects, the biggest value for me has been saving investigation time, reducing the need for separate tools, and improving my ability to identify suspicious activity..”

Edward Okereke

Cybersecurity Practitioner at Social Leader

[Read full review](#) 

Use Case

“The solution is used to learn how the tools work. It enables us to do consulting and demonstrate solutions. We develop attacks, detect them, and demonstrate how it works. The customers are interested in seeing how and what these tools can do..”

Jörg Kippe

Scientist at a educational organization with 10,001+ employees

[Read full review](#) 

“I have used Security Onion for learning purposes and for my own work, not as a reseller or a partner. My major use case with Security Onion was network scanning and network traffic analysis, including traffic capture and further analysis of that capture, detection, and scanning..”

Bhanwar Lal

Network Engineer at Crisp System India Pvt Ltd

[Read full review](#) 

“My main use case for Security Onion is monitoring components, including Zeek and Suricata, for training, as my environment runs on Proxmox and I use OpenSense as my firewall. I have also configured port mirroring on my Cisco switch to send network traffic for my lab VLANs to Security Onion for analysis.

“Currently, I am taking my master's degree and have set up some victim VMs that I use for testing in my lab with Security Onion, and I am using it towards my thesis paper..”

Matthew Sexton

Help Desk

[Read full review](#) 

“Security Onion is primarily used for network security monitoring, threat detection, log management, and centralized visibility across our infrastructure, serving as the primary means for our organization.

“Security Onion is used in our organization by continuously leveraging the Linux platform, Linux system, and network-based architecture to monitor threat detections and log management systems, which has proven very helpful for our organization in terms of network security monitoring..”

Hiten Nandasana

Angular developer at Flourish software

[Read full review](#) 

“I use Security Onion to view logs when students are working with different threats, as it has a dashboard that monitors logs, network traffic, and suspicious activities, which is the primary usage we employ.

The scenario I use for Security Onion in one of my classes is when we have a DDoS attack, and we start to monitor the DDoS attack under Security Onion to see if the network traffic related to the DDoS is coming to Security Onion and showing an alert or not.

One of the tools we regularly use through Security Onion is to show threats and suspicious activity by conducting port scanning and monitoring unusual connections, which allows students to identify red flags on Security Onion..”

Hamidreza Talebi

[Read full review](#) 

BCGEU Faculty, Computer Information Systems Administration at a educational organization with 1,001-5,000 employees

“My main use case for Security Onion is network analysis. I use Security Onion for network security monitoring, threat detection, and investigating suspicious activities. I use it to monitor traffic between Windows and Linux systems, analyze alerts, and identify potential security threats. For example, I have used Suricata to detect suspicious network activity, Zeek to examine connection logs, and Elastic Hunt to investigate alerts further. I have also used it to investigate port scans and failed login attempts. What I like most is that Security Onion brings these tools together in one platform, making it easier to investigate security events and understand what's happening across the network.

“I remember one situation that stands out when I was testing network security in my virtual environment. I used Kali Linux to perform a network scan against another system, and Security Onion detected the suspicious activity. I went into Security Onion, reviewed the Suricata alert, and used Zeek logs to examine the source and destination IP address, ports, and connection patterns. I also checked the packet capture to better understand what was happening. What I found was that the alerts were triggered by the scan I had performed rather than an actual attack. Security Onion helped me to connect the different pieces of evidence and understand why the activity was flagged. That experience really helped me to improve my investigation skills and learn how to distinguish suspicious activity from legitimate testing..”

Edward Okereke

Cybersecurity Practitioner at Social Leader

[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.

“I run Security Onion through private hardware on my server as a VM on several servers, specifically four, and it runs on my dedicated blue server where I host it myself..”

Matthew Sexton

Help Desk

[Read full review](#) 

“Security Onion's deployment needs to be a bit simple. Some explanations or jargon are a bit complicated and should be made simple enough to understand..”

Derek Maraw

Cyber Security Officer at AFC Holdings

[Read full review](#) 

“I think it is easy to install Security Onion; if a person knows how to install a virtual machine, they can easily install Security Onion as well. I have installed it multiple times, so it is easy, not tough..”

Bhanwar Lal

[Read full review](#) 

Network Engineer at Crisp System India Pvt Ltd

“The solution is partially in a real environment and partially in a virtual environment. The focus is on the OT environment. Our main focus is to deliver security in automation systems. It is very easy to set up..”

Jörg Kippe

[Read full review](#) 

Scientist at a educational organization with 10,001+ employees

“The installation process for Security Onion is very hard; if you do not know the Linux operating system and security monitoring tools very well, it is not going to be easy, and it is resource-intensive, requiring good CPU, memory, and storage for installation, which can be challenging for beginners..”

Hamidreza Talebi

[Read full review](#) 

BCGEU Faculty, Computer Information Systems Administration at a educational organization with 1,001-5,000 employees

“Security Onion can be made easier to set up initially, as it is somewhat difficult at the start, but once configured, it becomes a great tool to use.

“I assigned a rating of eight out of ten because the initial setup requires documentation reading and planning, which could be improved to make it easier for first-time users..”

Hiten Nandasana

Angular developer at Flourish software

[Read full review](#) 

Customer Service and Support

“I have not used customer support for Security Onion; however, I have participated in some community resources, and it is pretty good because it has a large community that has been around for years, which helps..”

Matthew Sexton

Help Desk

[Read full review](#) 

“We are part of the solution's blogging site, where we discuss with other people working on it so that we understand most things. Security Onion's blogging site or community forum helps us to resolve all our issues..”

Derek Maraw

Cyber Security Officer at AFC Holdings

[Read full review](#) 

Other Advice

“Security Onion is deployed on the cloud in our organization. I would recommend the solution to other users.

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

Anish Bajracharya

Postgraduate at a educational organization with 1,001-5,000 employees

[Read full review](#) 

“My advice depends on the requirements, network, and resources available in an organization. It also depends on whether someone is looking for a turnkey solution, whether they are interested in working alone, and what their skills are. There is no one solution for all installations. Overall, I rate the product a ten out of ten..”

Jörg Kippe

Scientist at a educational organization with 10,001+ employees

[Read full review](#) 

“I advise others looking into using Security Onion to set up a test environment to understand how it works and to explore its features, which helps in learning how to investigate logs and integrate additional tools before deploying it in a real environment. I rate Security Onion an eight out of ten because, among other competitors, Security Onion being open source provides an excellent learning opportunity for beginners to understand logs, detection, and investigation processes, leading to good outcomes in their skills development..”

Hamidreza Talebi

BCGEU Faculty, Computer Information Systems Administration at a educational organization with 1,001-5,000 employees

[Read full review](#) 

“Security Onion is a completely open-source and free platform, making it a cost-effective solution that works smoothly and effectively for our organization.

“Security Onion integrates well with our existing tools, primarily using Linux systems in our organization, allowing us to monitor logs and manage threat detection and operations in the public cloud effectively.

“Security Onion is very helpful in meeting compliance requirements and supports regular standards for our environment.

“I advise organizations that use Linux or have network security knowledge to consider Security Onion, as it satisfies requirements such as threat detection and log management systems.

“I would rate this review eight out of ten..”

Hiten Nandasana

Angular developer at Flourish software

[Read full review](#) 

“I would give Security Onion a rating of 10 out of 10. I have used other platforms, and I can tell that Security Onion provides powerful security monitoring and investigation tools in one platform, making it easier to manage. I particularly appreciate how Suricata, Zeek, and Elastic work together to help me detect suspicious activity, analyze network traffic, and investigate alerts. From my experience, it has made my investigations more organized and efficient. Although the initial setup can be challenging, the features and capability make it worthwhile.

“Regarding Security Onion's AI capabilities, I think Security Onion takes AI governance and security seriously, especially when it comes to controlling access and protecting sensitive information. I appreciate that Security Onion AI includes permission controls, so users can review and approve actions before the AI makes changes. It also provides administrative control and activity monitoring, which are important for accountability. I have not personally used some enterprise AI features, but based on my cybersecurity experience and the ones that I have used, I believe AI should assist analysts rather than make critical security decisions without human oversight. Overall, I think Security Onion has a good approach to AI governance. I would also like to see continued improvement in transparency, data privacy, and control over how AI handles sensitive security information.

“For the accuracy and reliability of output, I would say Security Onion definitely has very good security capability and has good potential to improve the speed and accuracy of security investigations. However, I believe the reliability of AI-generated results depends on the quality of the data being analyzed. I have not tested the AI features in an extensive way, so I cannot really give a precise accuracy rating for the particular AI that I have used. From my experience with Security Onion, I always verify findings against Suricata alerts, Zeek logs, and packet captures. I would take the same approach with AI-generated recommendations. I think AI is valuable for helping analysts identify suspicious patterns and understand alerts faster, but human verification is still important to avoid false positives or incorrect conclusions.

“My advice would be to first understand your network environment and make sure you have enough system resources. This is very important before installing Security Onion. I would also recommend starting with a small setup and gradually

expanding as you become more comfortable with the platform. From my experience, I learned how Suricata, Zeek, and Elastic work together. It is very important because it helps you investigate alerts more effectively. I would also encourage new users to take advantage of the documentation and practice analyzing real network traffic. Security Onion is an excellent solution for security monitoring and threat detection. There is a learning curve, especially during setup, but once you understand how the tools work together, it becomes very valuable..”

Edward Okereke

Cybersecurity Practitioner at Social Leader

[Read full review](#) 

“I would rate Security Onion an eight out of ten, as I think it is pretty good.

“I chose an eight because, as I mentioned, it takes a lot to get used to and learn, but I have not used anything else. Everything I have looked at suggests I should use Security Onion over something else first because it is good; it has everything together. Once you learn Security Onion, you can probably do most of the other things.

“I cannot comment on Security Onion's AI capabilities as it is a Security Onion Pro feature that I have not tested, since I am only using the free edition.

“From my experience using Security Onion in my home lab, the output from Zeek and Suricata is generally reliable, but it is important to understand what each tool is actually reporting. Zeek is particularly useful because it provides detailed information about network connections, DNS activity, and communication between devices, helping me understand what is happening across my different VLANs. Suricata is useful for detecting potential malicious activity through its detection rules, although not every alert indicates an actual security threat; false positives do occur. I think it is crucial to investigate alerts instead of automatically assuming they are accurate, as the reliability of the results depends heavily on how Security Onion is configured. For instance, if port mirroring is not configured

correctly or if the system is dropping packets, the information being analyzed might be incomplete. Overall, I would say I trust Security Onion as a network monitoring and detection platform, though I would not rely solely on alerts to make security decisions. The best approach is to correlate Zeek's network activity logs with Suricata's alert logs and investigate the evidence before making a final determination.

“My advice for others looking into using Security Onion is to have a solid understanding of networking fundamentals before diving in. You really need to grasp TCP/IP, VLANs, DNS, and how network traffic flows to make it much easier to understand what Security Onion is showing you. I would also recommend starting with a small lab environment instead of trying to monitor an entire network at once. That is what I have been doing with my Proxmox home lab, which has separate VLANs for my red team, blue team, and victim machines. Additionally, ensure you allocate enough hardware resources, particularly RAM, CPU, and storage, as I have faced a storage issue that caused my security interface to have faults. Learning Zeek and Suricata individually is important to understand the differences between network metadata and signature-based detection alerts. Do not assume every alert is a genuine threat; it is crucial to take the time to investigate the traffic and understand why an alert was generated. Primarily, I would tell beginners to be patient and take things one step at a time, as Security Onion has a learning curve but is a great platform for developing practical cybersecurity skills, especially if you are interested in working in a SOC or becoming a security analyst.

“I also recommend generating controlled test traffic and verifying that Security Onion actually captures it because just because the dashboard is running does not mean your monitoring configuration is working correctly.

“My overall rating for Security Onion is an eight out of ten..”

Matthew Sexton
Help Desk

[Read full review](#) 

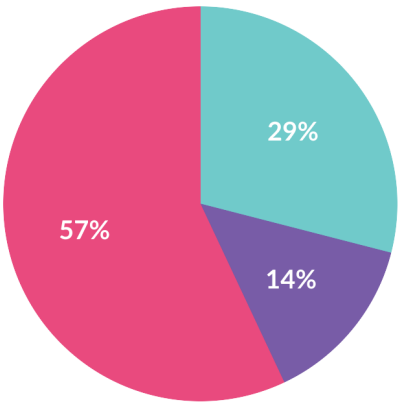
Top Industries

by visitors reading reviews

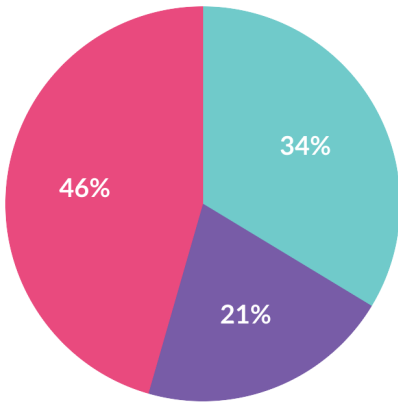


Company Size

by reviewers



by visitors reading reviews



Large Enterprise Midsized 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