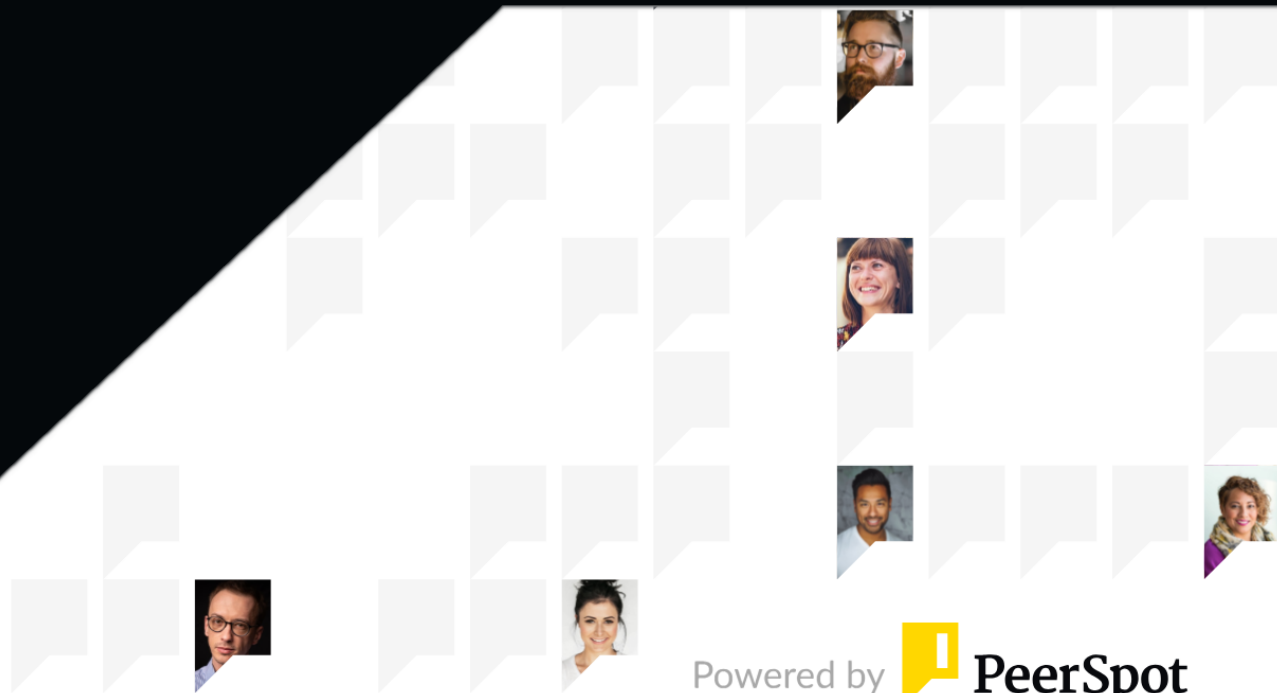


aws marketplace

Wazuh

Reviews, tips, and advice from real users



Powered by  PeerSpot

Contents

Product Recap..... 3 - 4

Valuable Features..... 5 - 9

Other Solutions Considered..... 10 - 12

ROI..... 13 - 14

Use Case..... 15 - 19

Setup..... 20 - 23

Customer Service and Support..... 24 - 25

Other Advice..... 26 - 28

Trends..... 29 - 30

About PeerSpot..... 31 - 32

Product Recap



Wazuh

Wazuh Recap

Wazuh offers an open-source platform designed for seamless integration into diverse environments, making it ideal for enhancing security infrastructure. Its features include log monitoring, compliance support, and real-time threat detection, providing effective cybersecurity management.

Wazuh stands out for its ability to integrate easily with Kubernetes, cloud-native infrastructures, and various SIEM platforms like ELK. It features robust MITRE ATT&CK correlation, comprehensive log monitoring capabilities, and detailed reporting dashboards. Users benefit from its file integrity monitoring and endpoint detection and response (EDR) capabilities, which streamline compliance and vulnerability assessments. While appreciated for its customization and easy deployment, room for improvement exists in scalability, particularly in the free version, and in areas such as threat intelligence integration, cloud integration, and container security. The platform is acknowledged for its strong documentation and technical support.

What are the key features of Wazuh?

- **MITRE ATT&CK Correlation:** Streamlines threat analysis by correlating security data with known attack patterns.
- **Log Monitoring:** Provides continuous oversight of log data to enhance security insights.
- **SIEM and ELK Integration:** Simplifies centralization of security events and analytics.
- **Kubernetes Support:** Ensures security measures align with containerized environments.
- **File Integrity Monitoring:** Alerts on unauthorized changes to critical files.
- **Endpoint Detection and Response:** Identifies and mitigates endpoint threats efficiently.
- **Compliance and Benchmarking:** Built-in rules assist in meeting regulatory standards.

What benefits and ROI should users look for?

- **Cost-Effectiveness:** Offers an affordable open-source security solution tailored for extensive customization.
- **Customization:** Users can adjust features to fit unique security requirements.
- **Scalability:** Facilitates growth by adapting to expanding security needs.
- **Comprehensive Support:** Backed by detailed documentation and technical expertise.
- **Regulatory Compliance:** Helps maintain adherence to industry-specific regulations.

In industries like finance, healthcare, and technology, Wazuh is utilized for its capabilities in log aggregation, threat detection, and vulnerability management. Companies often implement its features to ensure compliance with stringent regulations and to enhance security practices across cloud environments. By leveraging its integration capabilities, organizations can achieve unified security management, ensuring comprehensive protection of their digital assets.

Valuable Features

Excerpts from real customer reviews on PeerSpot:



“Wazuh caught my attention as a very cool solution for verifying file integrity.”



Sudarson Prabhu

Security Consultant at Payatu



“When we talk about functionality, the most valuable feature or function I have found in Wazuh is Wazuh EDR agent with EDR capabilities.”



MohamedAdel1

Tech Lead at a tech vendor with 51-200 employees



“I recommend Wazuh to everyone and believe more platforms, not just SIEM and XDR capability platforms, should be open source, allowing people to leverage these tools for the greater good.”

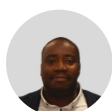


Verified user

Cyber Security Software Engineer at a tech services company with 11-50 employees



“Overall, I rate Wazuh a nine out of ten.”



Ebenezer Okoh

Security Consultant at ebenezer.okoh@agorasecurity.it



“Wazuh's most valuable features include file monitoring and compliance reporting, which do not require excessive costs.”



Sandip_Patel

Student at Dakota State University



“I would recommend Wazuh to others.”



Sean-Cox

Security Operations Center Analyst at [mailbox.org](https://www.mailbox.org)



“We found the MITRE framework mapping and the agent enrollment service to be the most valuable features of Wazuh.”



Verified user

Tech Lead at a tech vendor with 201-500 employees

What users had to say about valuable features:

“The valuable features of Wazuh include being open source and having the capacity to be used for anything desired. It allows for creating new automations, whereas other Software as a Service platforms have their own business models. With this open source tool, organizations can establish their own customized setup..”

Verified user

Cyber Security Software Engineer at a tech services company with 11-50 employees

[Read full review](#) 

“One of the most valuable features of Wazuh is its capability as a CVE helper. It assists in pulling reports about active CVEs in the system. Wazuh is a SIEM tool that is highly customizable and versatile. The fact that it is open source means it is always being expanded, which is beneficial for customizing solutions for individual client requests..”

Sean-Cox

Security Operations Center Analyst at mailbox.org

[Read full review](#) 

“The dashboards in Wazuh are very cool and they provided whatever data is required.

“I would give ten out of ten for the technical suggestion that I received from the documentation of Wazuh. The documentation provides everything that we are expecting. I have not tried any support from staff for Wazuh, but the documentation was very clear and I can give it ten out of ten..”

Sudarson Prabhu

Security Consultant at Payatu

[Read full review](#) 

“When we talk about functionality, the most valuable feature or function I have found in Wazuh is Wazuh EDR agent with EDR capabilities. This is the most valuable single feature in Wazuh – Wazuh agent capabilities.

“In my opinion, the main benefit Wazuh provides to users is visibility into user behavior. If you use it well, taking advantage of all agent features and capabilities, and using your own rules, it will give you full visibility of user behavior and user activity through the network or the environment..”

MohamedAdel1

Tech Lead at a tech vendor with 51-200 employees

[Read full review](#) 

“The threat hunting features of Wazuh are particularly valuable for our operations. We focus heavily on threat hunting capabilities to address potential threats before they become unmanageable.

“The intrusion detection capabilities integrate seamlessly with our existing firewall infrastructure. The system allows us to monitor endpoints effectively and collect security data that can be utilized across other platforms such as SOAR..”

Ebenezer Okoh

Security Consultant at ebenezer.okoh@agorasecurity.it

[Read full review](#) 

“Pricing-wise, Wazuh stands out, along with deployment flexibility and its documentation which is extremely good in comparison to Forti. The community support is also incredible.

“They have helped quite a bit because previously, we had a separate tool and management dashboard to do our compliance. With Wazuh, we receive that information without having to do anything extra. We just set up the SIEM and all of that information was automatically populated.

“The dashboards are very easy to understand and very quick with no lag or delay. I have experienced delays on Forti's dashboards, but not with Wazuh.

“Wazuh is quite good. In comparison to Forti, they are quite similar. They are very good at detection..”

Rajin Sandira

Engineer Information Security at N-Able (Pvt) Ltd

[Read full review](#) 

Other Solutions Considered

Wazuh can incorporate third parties and utilizes artificial intelligence for various features. Wazuh integrates effectively, deserving a solid 9 rating. That aspect is straightforward.

Verified user

Cyber Security Software Engineer at a tech services company with 11-50 employees

[Read full review](#) 

“We used Splunk primarily for log management purposes. There were no extra security modules or playbooks involved. We indexed the logs, built dashboards, generated reports, and set up alerts. That was the extent of our usage, without any additional security features..”

Muhammad Muaaz Bin Zaka

Software Engineer at a computer software company with 1,001-5,000 employees

[Read full review](#) 

“I did not use other SIEM solutions beforehand. Wazuh was already in use when I joined my organization. I am aware of Splunk, which is a commercial SIEM tool, yet have not used it..”

Godwin Edmond

Senior Security Information Analyst at Carbon MFB

[Read full review](#) 

“We evaluated LogRhythm, which is an excellent intelligence-based tool. However, it comes with a high cost for the intelligence features. Wazuh lacks AI or machine learning capabilities, but otherwise, it has all the necessary capabilities for a similar solution..”

Muhammad Muaaz Bin Zaka

[Read full review](#) 

Software Engineer at a computer software company with 1,001-5,000 employees

“Previously, I have used IBM QRadar, SentinelOne, and Splunk, which were all very expensive products.

My company started to use Wazuh considering its low prices compared to other solutions..”

PrzemekAndula

[Read full review](#) 

Cybersecurity specialist at a manufacturing company with 51-200 employees

“If you want to build it with an open-source SIEM solution, you can build it on QRadar or ELK, which are good options.

“Machine learning in Wazuh is very, very good, but for your knowledge, IBM QRadar significantly improved their UBA when it comes to machine learning and AI. Their focus is almost entirely on user behavior analytics. In QRadar, they concentrate on using machine learning algorithms and AI only for UBA..”

MohamedAdel1

Tech Lead at a tech vendor with 51-200 employees

[Read full review](#) 

ROI

Real user quotes about their ROI:

“The return on investment is visible in reduced mean time to detect from potentially three months to about an hour and mean time to respond from up to thirty days to two days..”

Verified user

[Read full review](#) 

Tech Lead at a tech vendor with 201-500 employees

“Due to confidentiality, I cannot share specific quantifiable benefits that deploying Wazuh has brought to my company. However, it resulted in cost reduction by avoiding lump sum payments and providing the benefit of having our own system..”

Verified user

[Read full review](#) 

Cyber Security Software Engineer at a tech services company with 11-50 employees

“I have seen value in security cost savings with Wazuh, as using proprietary EDR versions could save us substantial money, but I haven't made any comparisons since we started using Wazuh immediately..”

Ebenezer Okoh

Security Consultant at ebenezer.okoh@agorasecurity.it

[Read full review](#) 

“There is high potential for ROI, especially for small to medium businesses comparing Wazuh to market solutions. Wazuh offers more cost-effective options without compromising on security..”

Sandip_Patel

Student at Dakota State University

[Read full review](#) 

“I have a level three analyst on my team, and as a stock analyst, I am aware that they also offer an MSP program that provides partnership offerings and other related services. However, I am not very familiar with it..”

AKASH MAJUMDER

SOC Analyst at OVELOSEC

[Read full review](#) 

Use Case

“Wazuh is a SIEM platform with various applications in today's environment. Compliance checks have helped with regulatory requirements. I pulled in PCI DSS to check for file integrity monitoring. I completed one project where I removed malware..”

Verified user

Cyber Security Software Engineer at a tech services company with 11-50 employees

[Read full review](#) 

“We use Wazuh as a SIEM solution because it is open source, highly customizable, and continually expanding. Our clients can request various solutions for their issues, which Wazuh is able to address..”

Sean-Cox

Security Operations Center Analyst at mailbox.org

[Read full review](#) 

“Our organization is focusing on the integrity part for implementing Wazuh. We were checking solutions for File Integrity Monitoring systems that are available online. Wazuh caught my attention as a very cool solution for verifying file integrity. We decided to try Wazuh for focusing on the integrity part. While implementing it, our objective was achieved. We were able to monitor entire file integrity. Because our organization's business requires core concepts of integrity to be maintained, this was very important for us. Wazuh did this very well. We were not able to make it available to all endpoints. Instead, we tried it with servers. We changed our business requirements by storing all files that are processing into the server as a shared server and then we put File Integrity Monitoring and Wazuh in a single server. This worked out very well..”

Sudarson Prabhu

Security Consultant at Payatu

[Read full review](#) 

“I use Wazuh for daily security operations mainly on EDR endpoints by installing it on the agents that we are monitoring to collect security data. It helps us monitor endpoints and know what is going on at each endpoint, and we are able to tap the data and use it in other platforms such as SOAR.

“I find the threat hunting features of Wazuh most valuable, as we are more interested in the threat hunting side and want to move ahead into threat hunting before any threat becomes something that cannot be dealt with. Wazuh has a threat hunting functionality that we use extensively.

“The intrusion detection capabilities work effectively in my environment, as we also have firewalls, and we rely more on the firewall side for intrusion detection..”

Ebenezer Okoh

Security Consultant at ebenezer.okoh@agorasecurity.it

[Read full review](#) 

“At the moment, I'm working in software integration, so we are working with FortiGate. To research and get an idea, I did some investigation into Wazuh.

“They have already used Fortinet products.

“They use pretty much almost all Fortinet products including FortiGate, FortiSIEM, FortiXDR.

“At the moment, they only use FortiGate and FortiSIEM.

“I have worked with Wazuh before with limited experience..”

Rajin Sandira

Engineer Information Security at N-Able (Pvt) Ltd

[Read full review](#) 

“I have been working with Wazuh for two years, and I can explain how I use Wazuh. I did not use Wazuh as a SIEM solution. I use Wazuh as a tool for services we provide. This service is called compromise assessment. I use Wazuh because Wazuh agent has EDR agent capabilities and some EDR capabilities on their agents. I use Wazuh beside some tools in my toolset. I implement deception engines using it.

“Compromise assessment activity requires collecting logs and analyzing everything involved. Regarding threat detection capabilities, I speak honestly about it. When I say I use it for compromise assessment, I use it for that because Wazuh agent has great, very powerful capabilities to collect logs and correlate them against your environment to help detect threats or maybe future threats. Wazuh has an agent with EDR capabilities and some XDR capabilities also. That's why it's very good for me in terms of usage. It helps me in compromise assessment activity as a service we provide in our company.

“I find the real-time dashboard in Wazuh to be very good, but I do not recommend Wazuh for day-to-day operations. I recommend it for fast activities. I do not recommend Wazuh for long-term use or building your own SOC based on it..”

MohamedAdel1

Tech Lead at a tech vendor with 51-200 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.

“Initial setup was incredibly simple, requiring only the running of one script for a single node setup. Complexities arose during integration with Kubernetes-based workloads due to insufficient documentation..”

Verified user

[Read full review](#) 

Tech Lead at a tech vendor with 201-500 employees

“The initial setup is complicated. You need a specialist in the technology to make good use of it. You can do it on-premises. You can do it on Azure. You can do it on the hybrid cloud as a docker. So it's very flexible.

We use Azure, which we currently use as a single server. We will migrate it to our partner using Azure.

It takes two months to deploy completely..”

Renan Ruivo

[Read full review](#) 

IT Infrastructure at 4 Seniors Brasil

“The initial setup was not complex. We had prior experience with Elastic and Elk, so the deployment of Wazuh was quite familiar to us. It wasn't a major challenge.

However, we do need maintenance as we need to upgrade the version periodically. During maintenance, we have to switch off all the endpoints, turn off all the components, and then power off one by one to upgrade them to the latest version. This is done during a maintenance window.

One or two engineers are usually enough to handle the maintenance tasks..”

Muhammad Muaaz Bin Zaka

[Read full review](#) 

Software Engineer at a computer software company with 1,001-5,000 employees

“It is easy to install and deploy the tool, but only an experienced person can handle such areas. It means the subject matter expert can handle the tool. It cannot be given to someone randomly as the person needs to have some expertise.

The solution is easy to maintain.

Three people can deploy the solution.

Wazuh has given some timelines for the average deployment, but I must ask my team about it..”

NoorulHussain

[Read full review](#) 

CEO at Intrust Labs

“The initial setup was somewhat challenging for us, especially when we tried to do it independently. We faced some implementation issues but found solutions indicating ongoing product improvements. Sometimes, we face compatibility issues with certain industry products, requiring custom solutions, which can be a bit of a headache. However, we've managed to address these challenges over time. I would rate the setup process a five out of ten.

Wazuh is deployed on the cloud and on-premises in our customers' organisations. Deploying Wazuh depends on the customer's requirements; smaller customers take less time, but complex needs can extend the process. Typically, deployment is completed within a month..”

PubuduWijerathne

Systems Administration Engineer at 5G Networks Ltd

[Read full review](#) 

“Wazuh initial setup is very, very easy.

“In terms of deployment, I prefer to work on-premises. Here in Saudi Arabia, there are concerns about cloud services outside Wazuh country. They want everything in Wazuh cloud but inside Saudi Arabia, not outside it. For over five years, all my implementations have been on-prem. Now we only have Google Cloud and Alibaba Cloud; we still do not have Microsoft tenant availability in Saudi Arabia, but they claim it will be available next year. However, up until now, all my implementations are on-premises, and it's very, very easy and smooth..”

MohamedAdel1

[Read full review](#) 

Tech Lead at a tech vendor with 51-200 employees

Customer Service and Support

“I spoke with Wazuh support today regarding a quote. I would rate Wazuh support an 8 out of 10. They responded quickly, which was crucial as I was on a time constraint..”

Verified user

Cyber Security Software Engineer at a tech services company with 11-50 employees

[Read full review](#) 

“We use the open-source version of Wazuh, which does not provide paid support. Although the community is active, it is not highly responsive. Conversion from issue to resolution is average..”

Verified user

Tech Lead at a tech vendor with 201-500 employees

[Read full review](#) 

“Wazuh offers technical support, but you need to pay for it. If you are using the open-source solution, you'll need to rely on the extensive documentation and the community itself..”

Renan Ruivo

IT Infrastructure at 4 Seniors Brasil

[Read full review](#) 

“Customer service is excellent, rated a ten out of ten. Wazuh has a vast online community on platforms like Slack and Google groups. The response time for queries is great due to the extensive community support..”

Godwin Edmond

Senior Security Information Analyst at Carbon MFB

[Read full review](#) 

“I have not contacted the tool's support team. If my company contacts the product's support team, it would be easier for our company to deal with the product's areas like deployment and usage. In the upcoming year, I would like to use the commercial tech support offered by the product..”

PrzemekAndula

Cybersecurity specialist at a manufacturing company with 51-200 employees

[Read full review](#) 

“The technical support for Wazuh's licensed products is decent. Sometimes, there are delayed response and resolution times, which can be frustrating.

Wazuh is deployed on the cloud and on-premises in our customers' organisations. Deploying Wazuh depends on the customer's requirements; smaller customers take less time, but complex needs can extend the process. Typically, deployment is completed within a month..”

PubuduWijerathne

Systems Administration Engineer at 5G Networks Ltd

[Read full review](#) 

Other Advice

“I would recommend Wazuh to others. It is a good system that provides a comprehensive view of network activities when correctly set up with syslog and proper log injection. Overall, I would rate Wazuh an eight out of ten..”

Sean-Cox

Security Operations Center Analyst at mailbox.org

[Read full review](#) 

“I have not worked very well with Wazuh's threat detection capabilities because we already had some solution in place. Our focus was to implement Wazuh for integrity only and File Integrity Monitoring only. I have worked earlier with Wazuh and ManageEngine. When I was working with Wazuh, there was no artificial intelligence introduced. My overall review rating for Wazuh is eight out of ten..”

Sudarson Prabhu

Security Consultant at Payatu

[Read full review](#) 

“I would be willing to provide a review for products I have experience with. I recommend Wazuh to everyone and believe more platforms, not just [SIEM](#) and [XDR](#) capability platforms, should be open source, allowing people to leverage these tools for the greater good. I support it completely. Overall, I rate Wazuh 8 out of 10..”

Verified user

Cyber Security Software Engineer at a tech services company with 11-50 employees

[Read full review](#) 

“I do not work with Wazuh compliance management tools honestly.

“I cannot speak about Wazuh pricing for Wazuh paid version since I do not know Wazuh price. It's totally on Wazuh client side to purchase Wazuh product. I usually use Wazuh open-source or free version because my day-to-day activities only involve providing one service that's dependent on Wazuh called compromise assessment. I use Wazuh as part of my toolset for that purpose, which includes deception engines and other tools.

“My overall review rating for Wazuh is seven..”

MohamedAdel1

Tech Lead at a tech vendor with 51-200 employees

[Read full review](#) 

“Right now, we haven't decided. We just want to explore and see what is available.

“I prefer Wazuh a bit more, though both are similar.

“I would rate Wazuh eight to nine out of ten.

“I would rate Forti seven to eight out of ten.

“Wazuh is actually better than Forti.

“I have utilized the solution.

“My overall rating for Wazuh is 9 out of 10..”

Rajin Sandira

Engineer Information Security at N-Able (Pvt) Ltd

[Read full review](#) 

“I have not seen Wazuh moving in the direction of AI-driven threat detection projects myself, but since the market is moving that way, I wouldn't be surprised if they implemented it soon.

“My plans to increase the usage of Wazuh or switch to another tool depend on what my boss decides.

“We don't refer to any community support specifically, as we rely on other platforms such as [GitHub](#) or Discord, depending on the application.

“I recommend that as more companies come on board with Wazuh, it will motivate those who contribute to it, but I am also cautious that as it gains attention, a large company might buy it and change its course of business.

“Overall, I rate Wazuh a nine out of ten..”

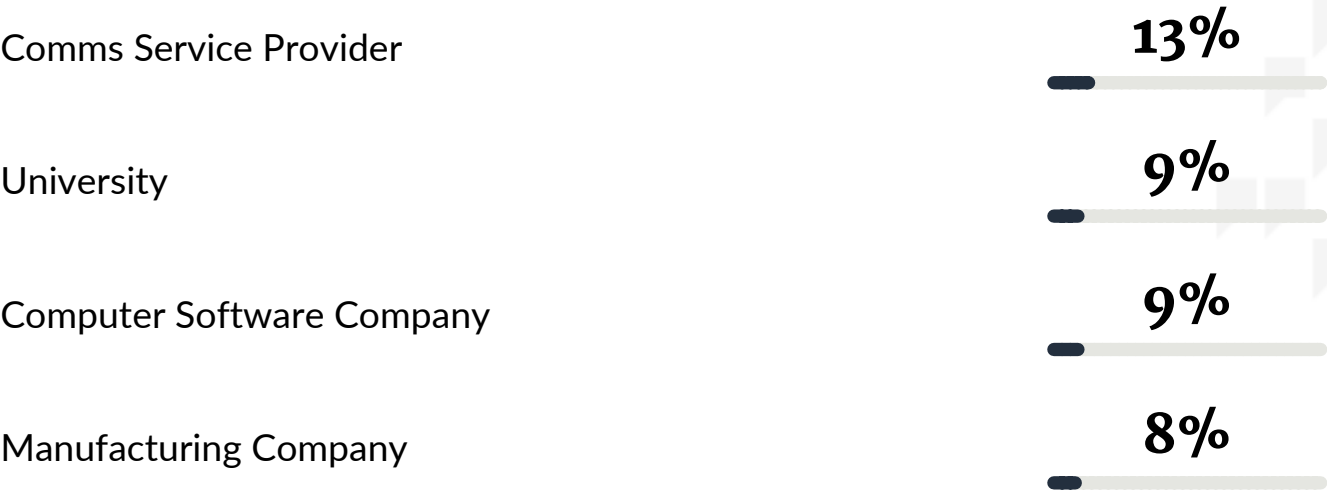
Ebenezer Okoh

Security Consultant at ebenezer.okoh@agorasecurity.it

[Read full review](#) 

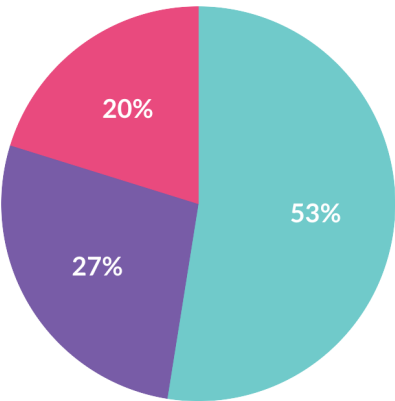
Top Industries

by visitors reading reviews



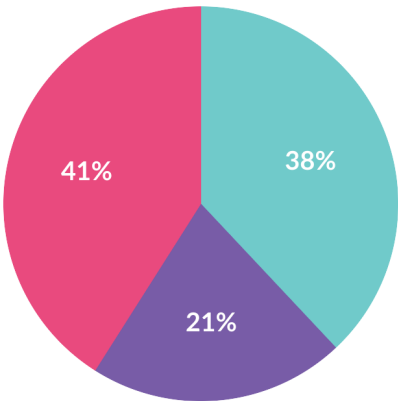
Company Size

by reviewers



Company Size

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