aws marketplace

Wazuh

Reviews, tips, and advice from real users

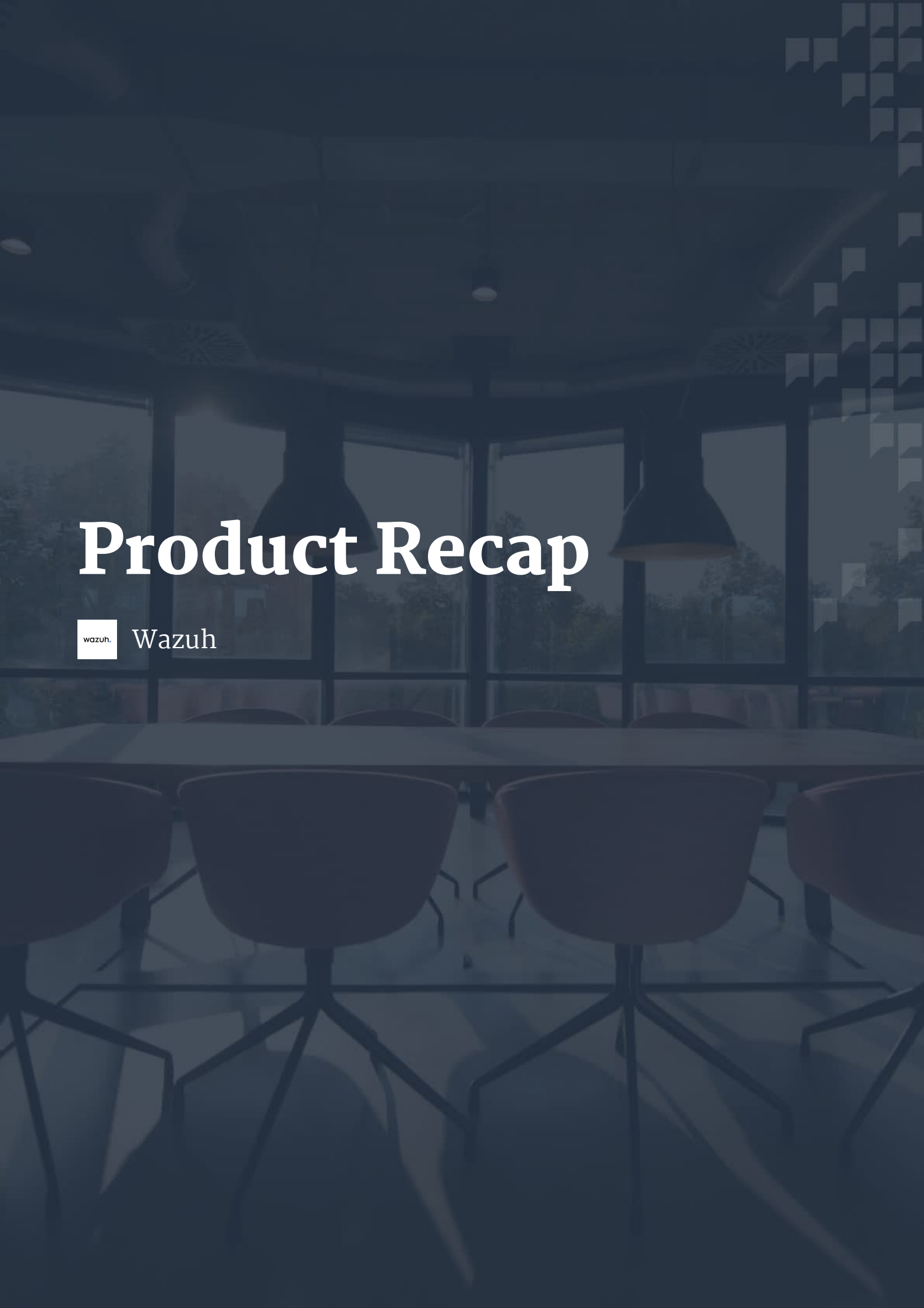





Powered by PeerSpot

Contents

©2025 PeerSpot, All Rights Reserved



Product Recap

Wazuh

Wazuh Recap

Wazuh offers comprehensive security features like MITRE ATT&CK correlation, log monitoring, and cloud-native infrastructure. It ensures compliance and provides intrusion detection with high scalability and open-source flexibility, ideal for businesses seeking robust SIEM capabilities.

Wazuh stands out in security information and event management by providing efficient log aggregation, vulnerability scanning, and event correlation against MITRE ATT&CK. Its capability to integrate seamlessly with environments, manage compliance, and monitor files makes it suitable for cloud-native infrastructures and financial sectors. Despite its technical support needing enhancement and opportunities for improving AI integration and threat intelligence, its open-source nature and cost-effectiveness make it appealing. Users can leverage custom dashboards powered by Elasticsearch for precise data analysis, even though there is a desire for a more user-friendly interface and better enterprise solution integration. Deployment may be complex, but its features contribute significantly to fortified security postures.

What are the essential features of Wazuh?

- MITRE ATT&CK Correlation: Aligns events with recognized adversary tactics and techniques.
- Log Monitoring: Collects and analyzes logs for threat detection.
- Cloud-Native Infrastructure: Supports modern cloud environments.
- Vulnerability Scanning: Identifies potential security weaknesses.
- File Integrity Monitoring: Ensures the integrity of sensitive files.
- Open-Source Flexibility: Customizable and adaptable code base.

What benefits should users consider?

- Cost-Effectiveness: Offers a budget-friendly security solution.
- Ease of Use: Simplified setup and management.
- Comprehensive Compliance Management: Aids in meeting regulatory requirements.
- High Scalability: Grows with businesses and adapts to different environments.
- Extensive Third-Party Integrations: Connects to various existing systems.

Industries like finance and cloud infrastructure heavily utilize Wazuh for its security strengths. By monitoring endpoints and ensuring compliance with frameworks, companies can improve security posture and swiftly detect anomalies. The platform's focus on event correlation and alerts for security incidents is particularly beneficial.

©2025 PeerSpot, All Rights Reserved

Valuable Features

Excerpts from real customer reviews on PeerSpot:

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

Ebenezer Okoh

Security Consultant at ebenezer.okoh@agorasecurity.it

- “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

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

Sandip_Patel

Student at Dakota State University

©2025 PeerSpot, All Rights Reserved

"The product's initial setup phase was easy."

Muhammad_Saad

Software Engineer at i2c Inc.

"I would recommend Wazuh to others."

Sean-Cox

Security Operations Center Analyst at 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

"The most valuable feature of Wazuh is its EDR capabilities."

Godwin Edmond

Senior Security Information Analyst at Carbon MFB

©2025 PeerSpot, All Rights Reserved

What users had to say about valuable features:

"The most valuable features include file integrity monitoring, Wazuh engines, Wazuh rulesets (including rulesets for Apache and firewall routers), and vulnerability detection.."

Muhammad Muaaz Bin Zaka
Software Engineer at a computer software company with 1,001-5,000 employees

Read full review

"The most valuable feature of Wazuh is its EDR capabilities. It operates in a server-agent mode, which allows us to aggregate logs from endpoints and monitor server activities, such as vulnerability scans and compliance checks. Wazuh is open to numerous integrations with third-party tools like forensics tools, adding to its versatility.."

Godwin Edmond
Senior Security Information Analyst at Carbon MFB

Read full review

©2025 PeerSpot, All Rights Reserved

“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

“Wazuh's most valuable features include file monitoring and compliance reporting, which do not require excessive costs. These aspects are vital as they provide alerts for changes and facilitate the monitoring of compliance. The platform is also relatively easy to set up and operate. Reports are straightforward to extract and prove useful for compliance requirements..”

Sandip_Patel

Student at Dakota State University

Read full review

©2025 PeerSpot, All Rights Reserved

"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 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

©2025 PeerSpot, All Rights Reserved

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

©2025 PeerSpot, All Rights Reserved

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

Read full review

"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
Cybersecurity specialist at a manufacturing company with 51-200 employees

Read full review

"We evaluated Google Chronicle and Elastic-based SIEM (ELK SIEM), but Wazuh was the most cost-effective solution, being open-source with necessary compute infrastructure.."

Verified user
Tech Lead at a tech vendor with 201-500 employees

Read full review

©2025 PeerSpot, All Rights Reserved

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
Tech Lead at a tech vendor with 201-500 employees

Read full review

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

Read full review

©2025 PeerSpot, All Rights Reserved

"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

©2025 PeerSpot, All Rights Reserved

Use Case

"We are using Wazuh for security information and event management, PCI DSS compliance, auditing, real-time sensitive monitoring, and meeting regulatory requirements.."

Muhammad Muaaz Bin Zaka

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

Read full review

"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

©2025 PeerSpot, All Rights Reserved

"I am currently evaluating and using Wazuh for file monitoring and compliance reporting. We are in the process of conducting a POC to understand how the rules work. I lead this effort to explore and evaluate Wazuh as part of my learning and work experience.."

Sandip_Patel
Student at Dakota State University

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

©2025 PeerSpot, All Rights Reserved

"Our primary use case was around data collection and anomaly detection. We integrated Wazuh with Google Cloud and other cloud providers to receive alerts and insights if there is any unauthorized data access in the production environment.

We also monitor virtual machines for any malicious command execution and get notifications for any privilege access attempts. Additionally, we detect anomalies in traffic patterns related to specific client accounts.."

Verified user

Tech Lead at a tech vendor with 201-500 employees

Read full review

©2025 PeerSpot, All Rights Reserved

"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

©2025 PeerSpot, All Rights Reserved

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

Tech Lead at a tech vendor with 201-500 employees

Read full review

"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

IT Infrastructure at 4 Seniors Brasil

Read full review

©2025 PeerSpot, All Rights Reserved

"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

©2025 PeerSpot, All Rights Reserved

“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

©2025 PeerSpot, All Rights Reserved

“If one is difficult and ten means an easy setup phase, I rate the product's initial setup phase a seven out of ten. The product's initial setup phase was easy.

I have not faced any challenges during the product's installation phase. I was unable to change the admin password. The default admin password for admins couldn't be changed, and I am still unable to change my password because it does not allow me to change its admin password.

I was involved directly in the deployment process.

The solution is deployed on an on-premises model.

The solution can be deployed in a single day..”

Muhammad_Saad

Software Engineer at i2c Inc.

Read full review

©2025 PeerSpot, All Rights Reserved

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

©2025 PeerSpot, All Rights Reserved

“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

©2025 PeerSpot, All Rights Reserved

Other Advice

"I would recommend Wazuh. It's a valuable tool for security operations. On a scale of one to ten, I currently rate Wazuh as a six. I may rate it higher after more experience.."

Sandip_Patel
Student at Dakota State University

Read full review

"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

©2025 PeerSpot, All Rights Reserved

"Wazuh is well-suited for small to medium-sized organizations seeking better data and security visibility for a reasonable investment. There is a learning curve due to less comprehensive documentation, but it is a beautifully designed solution.

I'd rate the solution seven out of ten.."

Verified user
Tech Lead at a tech vendor with 201-500 employees

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 would advise you to carefully follow the documentation. It is straightforward and to the point. If any issues arise, the Wazuh Slack community is highly active and responsive. They can provide assistance within 24 hours or even less, helping with any deployment or management challenges.

Wazuh offers numerous features, such as the ability to define custom rules for detecting malicious activities and remembering behaviors. Unlike some paid tools, Wazuh is extensive and extendible and allows integration with open-source tools and scripts. It is flexible, reliable, and open-source, which is its biggest advantage.

©2025 PeerSpot, All Rights Reserved

Overall, it is a good solution. I would rate the solution a nine out of ten. Considering that Wazuh is open source and free of cost while providing all the necessary features, I would rate it nine or ten. I lean towards ten because it offers a comprehensive solution without any financial burden. However, compared to industry leaders like LogRhythm and Splunk, which have machine learning modules, Wazuh lacks in that aspect. So, overall, I would rate it nine, but because of its cost-effectiveness, it deserves a ten.."

Muhammad Muaaz Bin Zaka
Software Engineer at a computer software company with 1,001-5,000 employees

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

©2025 PeerSpot, All Rights Reserved

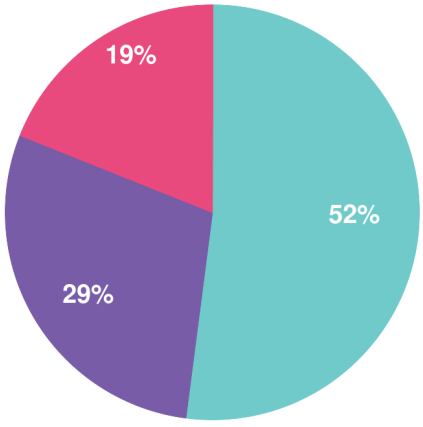
Top Industries

by visitors reading reviews

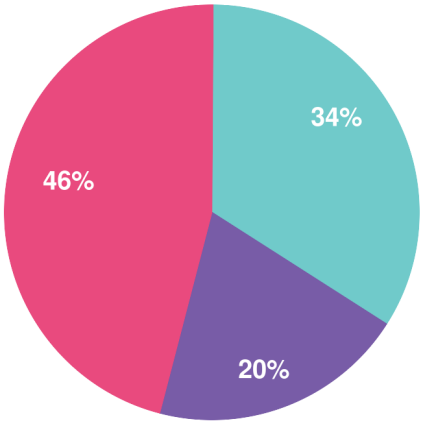
Computer Software Company	15%
Comms Service Provider	9%
University	8%
Manufacturing Company	7%

Company Size

by reviewers



by visitors reading reviews



Large Enterprise Midsize Enterprise Small Business

©2025 PeerSpot, All Rights Reserved

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

©2025 PeerSpot, All Rights Reserved

About PeerSpot

PeerSpot is the leading review site for software running on AWS and other platforms. We created PeerSpot to provide a trusted platform to share information about software, applications, and services. Since 2012, over 22 million people have used PeerSpot to choose the right software for their business.

PeerSpot helps tech professionals by providing:

- A list of products recommended by real users
- In-depth reviews, including pros and cons
- Specific information to help you choose the best vendor for your needs

Use PeerSpot to:

- Read and post reviews of products
- Access over 30,000 buyer's guides and comparison reports
- Request or share information about functionality, quality, and pricing

Join PeerSpot to connect with peers to help you:

- Get immediate answers to questions
- Validate vendor claims
- Exchange tips for getting the best deals with vendor

Visit PeerSpot: www.peerspot.com

PeerSpot

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

reports@peerspot.com

+1 646.328.1944

©2025 PeerSpot, All Rights Reserved