



Graylog Enterprise

Reviews, tips, and advice from real users



Powered by  **PeerSpot**

Contents

Product Recap..... 3 - 4

Valuable Features..... 5 - 11

Other Solutions Considered..... 12 - 14

ROI..... 15

Use Case..... 16 - 20

Setup..... 21 - 23

Customer Service and Support..... 24 - 26

Other Advice..... 27 - 30

Trends..... 31 - 32

About PeerSpot..... 33 - 34

Product Recap



Graylog Enterprise

Graylog Enterprise Recap

Graylog Enterprise, recognized for log collection, real-time search, and enriched data handling, offers an open-source framework that integrates seamlessly with Elasticsearch. Its user-centric interface streamlines data correlation and log aggregation, supporting both backend services and comprehensive monitoring needs.

Graylog Enterprise stands out for its stability and powerful log management capabilities, facilitating efficient log aggregation, real-time updates, and data analytics. Users benefit from its plugin-based alerting, user-friendly interface, and support for microservices, including Docker integration. The ability to search in detail, flexible API integration, and data enrichment features are highly valued. Challenges include collector application issues, desired visualization enhancements, and authentication integration improvements. Users seek advancements in UI customization, backup functions, and easier rule creation.

What are Graylog Enterprise's most important features?

- **Log Collection:** Efficiently aggregates and handles diverse logs.
- **Real-Time Search:** Provides immediate log data access.
- **Custom Alerts:** Plugin-based alerting for tailored notifications.
- **Dashboard Enhancements:** Improved visualization for data insights.
- **Data Enrichment:** Adds value through detailed log analysis.

What benefits and ROI can users expect?

- **Audit Trail Support:** Essential for compliance in financial sectors.
- **Security Event Correlation:** Enables incident analysis and response.
- **Faster Issue Identification:** Speeds up troubleshooting with detailed visualization.
- **API Flexibility:** Seamless integration across systems and environments.
- **Comprehensive Monitoring:** Centralized log management enhances oversight.

In industrial use, Graylog Enterprise is crucial for audit trailing in financial sectors, facilitating security event identification and error monitoring. Backend teams leverage real-time analytics for swift issue resolution, while developers appreciate the comprehensive log visualization enabled by Docker integration for microservice management.

Valuable Features

Excerpts from real customer reviews on PeerSpot:



“It is easier to find some issues, and if I find some issues, then it is easier to resolve them.”



Nicolae Clornii

Security Officer at JSC "Moldtelecom" S.A.



“Graylog Enterprise positively impacts the organization by helping the team and analysts investigate incidents faster since logs from servers, endpoints, cloud, and firewalls are available in one place.”



Vikram Chakravarthy

Cyber Security Engineer II (Vulnerability & Threat Management) at FICO



“With Graylog Enterprise, monitoring improved by up to 80 percent because of having all the logs centralized.”



Verified user

Platform Engineering at a comms service provider with 1,001-5,000 employees

- ✓ “Graylog Enterprise has positively impacted my organization by significantly minimizing our workload and making it easier to identify any issues in a service.”



Verified user

Junior Dev Ops Engineer at a consultancy with 11-50 employees

- ✓ “The Graylog features that have proven to be most beneficial for our data analysis in particular are that we tend to use it as a big data store, so we have the correlation rules that, if something matches under certain conditions, it raises an alarm.”



Verified user

Head of Cyber Security & CTO at a tech services company with 51-200 employees

- ✓ “It has data adapters and lookup tables that utilize HTTP calls to APIs.”



Atassi Kalo

Security Analyst at Netsharqs cybersecurity GmbH

- ✓ “Troubleshooting is straightforward with Graylog Enterprise.”



Gavrav Pawar

Dev Ops Team's Lab at a consultancy with 11-50 employees

What users had to say about valuable features:

“I would say log enrichment via these data adapters and lookup tables is valuable, especially the caching ability since Graylog doesn't always have to make API calls for every single instance if it is enriching the same value. That is very handy and makes it scalable..”

Atassi Kalo

Security Analyst at Netsharqs cybersecurity GmbH

[Read full review](#) 

“The features and capabilities of Graylog that we have found most valuable are related to its basis on open search, which was Elasticsearch. We appreciate being able to integrate custom feeds and do custom parsers, and to be able to do some of the correlation on it. That all works effectively. The Graylog features that have proven to be most beneficial for our data analysis in particular are that we tend to use it as a big data store, so we have the correlation rules that, if something matches under certain conditions, it raises an alarm. We use it for investigating problems and problem management. We throw all the information at it, we have it alerting for certain conditions, but generally we use it for deep diving into issues as needed..”

Verified user

Head of Cyber Security & CTO at a tech services company with 51-200 employees

[Read full review](#) 

“The standout features that make Graylog Enterprise valuable for my team are particularly helpful for Site Reliability Engineers, IT, and DevOps security, as it delivers excellent functionality without extreme cost. Its alerting system and notification capabilities really help us, as we use Slack to receive alerts from Graylog Enterprise. Additionally, the data management and the pipeline to transform and categorize the logs as they flow in are valuable. The best feature of Graylog Enterprise is its high-performance search engine that provides fast, flexible, and scalable analysis of machine data or pod data.

“When there is any error, bug, or downtime, Graylog Enterprise sends us an alert to Slack, so we can immediately investigate and find what the issue is, whether it is with the pipeline or within a service. We can determine exactly what happened and why it is causing the downtime. If we need to spin up more pods or if it needs more memory or CPU usage, we take the appropriate initiative based on that assessment.

“Graylog Enterprise has positively impacted my organization by significantly minimizing our workload and making it easier to identify any issues in a service. It features good custom dashboards, visualization, and good search capability as well..”

Verified user

[Read full review](#) 

Junior Dev Ops Engineer at a consultancy with 11-50 employees

“It is easier to find some issues, and if I find some issues, then it is easier to resolve them. It is not so difficult.

“We stopped using Graylog Enterprise because we found some issues with logs that came through, and they were too difficult to parse. We saw that it was better to use Splunk. It is better because it has an analysis algorithm and can also draw graphics with some help with this. To use Graylog Enterprise, we needed to import another system that collects and correlates the logs to see the statistics.

“I did not find the alerting systems in Graylog Enterprise adequate to maintain operational efficiency. It was acceptable, but our company is developing, so we needed to improve and see different analysis and different ways to see the data. For this reason, we decided to buy a new SIEM platform where we could improve some additional features..”

NicolaeClornii

Security Officer at JSC "Moldtelecom" S.A.

[Read full review](#) 

“In my experience, if I compare Graylog Enterprise with the ELK stack, I can see that Graylog is way easier to set up and has a great, good-looking UI. These are the things where I could see Graylog as a lightweight tool with more flexibility in terms of setting it up compared to alternatives such as ELK.

“In the case of Elasticsearch, multiple separate components are needed. However, in the case of Graylog Enterprise, there was only one binary that we used to install on the machines.

“Graylog Enterprise has positively impacted my organization by enhancing visibility through improved monitoring capabilities and getting logs from all the machines, which contributed to enhanced visibility and monitoring. We had over 500 virtual machines, and monitoring the logs by going to each virtual machine was tedious in the past. With Graylog, all the logs from those 500 machines were centralized in one Graylog Enterprise system. From there, it was very easy to query the logs and see the patterns, and thus the monitoring was significantly enhanced.

“With Graylog Enterprise, monitoring improved by up to 80 percent because of having all the logs centralized. Users or engineers would not have to SSH on each node to see the logs, meaning monitoring or visibility got improved by 80 percent or more..”

Verified user

[Read full review](#) 

Platform Engineering at a comms service provider with 1,001-5,000 employees

“The best feature Graylog Enterprise offers is its centralized log management, allowing analysts to search logs from a single tool instead of checking multiple tools. It is fast, and we can search effectively because during incident response time, the SOC analyst can quickly search a suspicious IP, username, or any IOCs across the historical logs. Another valuable aspect is the alerting and correlation functionality, where alerts can be created for multiple rules based on use cases, such as multiple failed logins, privilege escalation, abnormal authentication behavior, and other security events.

“The dashboard and visualization in Graylog Enterprise is good for SOC monitoring purposes.

“Graylog Enterprise positively impacts the organization by helping the team and analysts investigate incidents faster since logs from servers, endpoints, cloud, and firewalls are available in one place. Instead of switching between multiple tools, timelines can be reviewed and suspicious activity validated quickly, resulting in faster investigation times, better visibility into logs, and improved incident response capabilities. This has also reduced manual effort and compliance tasks.

“Previously, as an SMB company, approximately 40 to 50 alerts per day were generated. When Graylog Enterprise was implemented and evaluated, it correlated everything, providing true positive alerts and reducing the number of alerts to 10, which allows analysts to monitor those true positive alerts and take action accordingly..”

Vikram Chakravarthy

Cyber Security Engineer II (Vulnerability & Threat Management) at FICO

[Read full review](#) 

Other Solutions Considered

“I previously used Splunk and ELK as well, but they were with a different employer. It was never a situation where Graylog Enterprise was introduced as a replacement for other tools; the employer I was talking about was primarily using it..”

Verified user

Platform Engineering at a comms service provider with 1,001-5,000 employees

[Read full review](#) 

“Previously, Elasticsearch, an open-source SIEM tool, was used, and multiple monitoring approaches were evaluated depending on maturity and requirements..”

Vikram Chakravarthy

Cyber Security Engineer II (Vulnerability & Threat Management) at FICO

[Read full review](#) 

“The organization often compares Graylog Enterprise with other SIEM and detection solutions tools based on the integration, and it is upon leadership's decision..”

Vikram Chakravarthy

Cyber Security Engineer II (Vulnerability & Threat Management) at FICO

[Read full review](#) 

“We stopped work with Graylog Enterprise and now we use another SIEM platform. We do not use Graylog Enterprise anymore. We stopped using Graylog Enterprise and switched to Splunk about seven to eight months ago..”

NicolaeClornii

Security Officer at JSC "Moldtelecom" S.A.

[Read full review](#) 

“Evaluating other options before choosing Graylog was somewhat straightforward because we've been using it for some time and are confident with it. Originally, we recommended Graylog to a customer, but they chose QRadar, which is very expensive and didn't scale as effectively. Eventually, we put Graylog next to QRadar because QRadar couldn't keep up..”

Verified user

Head of Cyber Security & CTO at a tech services company with 51-200 employees

[Read full review](#) 

“I used Graylog until a few months ago, and I'm currently using Sentry. With Sentry it is quite easy to filter, for example, errors for a specific project just by clicking a drop down. On Graylog, we had to perform active filtering through the search bar. The filtering process was a bit different. I wouldn't say they differ too much, but Sentry also allows me to do some bug tracking and mark them like, "Okay, now I have to review this," or "This has been resolved", which is not something I would ask for in a log tool, but it's available..”

Jonas Leeb

Software Engineer & Co-Founder at Plexify GmbH

[Read full review](#) 

ROI

Real user quotes about their ROI:

“Instead of having five analysts working, Graylog Enterprise has reduced the number of analysts as well as time, resulting in a decreased cost of 20%. It has provided better quality and improved detection capabilities..”

Vikram Chakravarthy

Cyber Security Engineer li (Vulnerability & Threat Management) at FICO

[Read full review](#) 

“The return on investment or cost savings we have seen since the deployment of Graylog is primarily in time savings, allowing our security team and IT engineers quick access to information, as it all goes to one place. It makes it quite quick to find things, enabling us to retrieve the information needed to respond swiftly..”

Verified user

Head of Cyber Security & CTO at a tech services company with 51-200 employees

[Read full review](#) 

Use Case

“We describe our customers' usual use cases for Graylog as one where we use it for event correlation. We take typical IT events, and we also use it for security event correlation as well. So, both security and general IT. We use Graylog internally in our company..”

Verified user[Read full review](#) 

Head of Cyber Security & CTO at a tech services company with 51-200 employees

“I mostly use it for log management, log aggregation, and visualization. In my case, I am researching how to basically integrate cyber threat intelligence into open-source team systems.

Graylog is very handy. It has data adapters and lookup tables that utilize HTTP calls to APIs. I can enrich data by automating HTTP calls to a MISP instance, for example, or other threat feeds. This is basically the brunt of the work. Otherwise, normalization and parsing of logs from different sources are involved..”

Atassi Kalo[Read full review](#) 

Security Analyst at Netsharqs cybersecurity GmbH

“I remember using Graylog Enterprise in the past at a software house where we used it for logging. During that time, we were using Graylog Enterprise as a log aggregator, collecting logs from multiple systems and then exporting and visualizing them within Graylog.

“We had multiple Linux-based machines, and we were trying to capture the logs from the systems and export them into Graylog so that they could be centrally visualized. Graylog Enterprise was deployed on-premises in a private cloud..”

Verified user

[Read full review](#) 

Platform Engineering at a comms service provider with 1,001-5,000 employees

“Graylog Enterprise is the logging and management tool we initially used, but later we stopped using it and switched to Loki, Grafana Loki for the logs. Eventually, we moved back to Graylog Enterprise after approximately one year.

“The main use case for Graylog Enterprise is that we primarily use it for our enterprise logs. We have around 11 services, so we use it to collect all of our logs in one location. We use it for both QA and production environments.

“A specific example of how we use Graylog Enterprise in our environment is that we have multiple logins for our MDM solution, a mobile device management solution. Since it is an enterprise application, we generally use Graylog to retrieve the logs and determine if there is an error or any downtime. Graylog Enterprise has been very helpful in identifying issues and is also extremely valuable for handling high-volume log throughput. The cost-effectiveness of Graylog Enterprise has been particularly beneficial to us..”

Verified user

[Read full review](#) 

Junior Dev Ops Engineer at a consultancy with 11-50 employees

“Graylog Enterprise is used primarily for log management and to perform security analytics. It helps the organization collect logs from different sources and centralize them in one place. We can search and analyze events, detect suspicious activity, and it supports security investigations. The organization ingests a lot of logs including firewall logs, AWS, Windows endpoints, and authentication logs. It helps collect everything in a single dashboard, and we can search the logs and monitor each aspect.

“Graylog Enterprise collects everything in one dashboard, allowing the SOC team to search the logs and monitor every alert based on the rules, enabling investigation of suspicious activity. For example, if a user account suddenly logs in from an unusual or unauthorized location with multiple failed login attempts, Graylog helps correlate those logs and allows analysts to investigate that quickly.

“Graylog Enterprise is used for compliance and audit log retention, for investigation, and it is useful for centralized log collection.

“In alerting and correlation, logs are ingested from multiple sources, allowing us to create alerts based on those use cases. For example, if a suspicious IP from an unauthorized location is detected, the IP is checked in the firewall logs, application logs, or whether it has executed some PowerShell script or is showing some authentication behavior. Based on that, everything is correlated, and those insights are available in the tool for SOC analysts to analyze those alerts..”

Vikram Chakravarthy

Cyber Security Engineer II (Vulnerability & Threat Management) at FICO

[Read full review](#) 

“We have various environments, including UAT, SIT, Dev, and Production, with automated deployments. We refer to Graylog Enterprise to verify if deployments have completed, check their status if they have failed, and determine what version is currently running.

“Some team members from the QA team are unable to see the exact version or the newer version. We use Graylog Enterprise to check if the deployment is done, identify what version has been deployed, and determine on what date the environment was updated.

“We provide variables to fit in the relevant section and select the appropriate one, such as the environment and what we need to check. This is the main feature I appreciate about Graylog Enterprise. Whatever we select, such as the database name or environment name, all the information appears, including the date of the last deployment and related details.

“Troubleshooting is straightforward with Graylog Enterprise. Whenever we encounter an issue, whether from the QA team or other team members, we use it to troubleshoot the specific problem and implement a fix.

“During deployments, we fix issues as quickly as possible using Graylog Enterprise. When team members from the QA team inform us that something is not working or an environment is down, we access Graylog Enterprise to verify if the deployment has been completed and check exactly what version is running.

“We receive approximately 15 to 16 daily requests, and we resolve them through Graylog Enterprise..”

Gavrav Pawar

Dev Ops Team's Lab at a consultancy 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.

“Configuring the SSL certificates usually takes a lot of time because I have to add the certificate to the Java keystore in a very specific format. Otherwise, it doesn't get recognized. It is not very convenient. That took me about one week to figure out..”

Atassi Kalo

Security Analyst at Netsharqs cybersecurity GmbH

[Read full review](#) 

“The initial setup was complex. The deployment process involved server configuration, setting up alerts, and configuring the system. When upgrading from version 4.2 to 5.1, the configuration took some time..”

Nicolae Clornii

Security Officer at BC Energbank S.A.

[Read full review](#) 

“We have top-level engineers, and we didn't have any problems at all, but any random guy could also set it up. It involved the magic of regular Linux commands. It was pretty easy. I would rate it a five out of five in terms of the ease of the setup. It's great..”

Andrey Mostovykh

[Read full review](#) 

Senior Data Architect at a non-tech company with 201-500 employees

“Graylog Enterprise is a security product and generally requires an evaluation. Multiple tools were evaluated, and the solution will need to be scaled if required, as the main cost depends on integration and operation requirements. These details will be shared with leadership, and they will make the decision..”

Vikram Chakravarthy

[Read full review](#) 

Cyber Security Engineer II (Vulnerability & Threat Management) at FICO

“It really depends. If you're going to slap Graylog into a very small environment and do a standalone instance, it's super easy and straightforward. You have to install Mongo, Elasticsearch, and Graylog and connect them to each other, which is super simple. There are tons of easy tutorials online available to help you do that.

However, if you want to set up a highly scalable cluster, things will get a little bit complex. It's still very manageable, but it's definitely complex..”

Peter Malaty

[Read full review](#) 

Sr. DevOps Engineer at TechStyle Fashion Group

“I would rate my experience with the initial setup of Graylog on a scale of 1 to 10 as probably about a five. If someone has never used Linux before, it would be very difficult, but if you're familiar with Linux and the day-to-day things behind the scenes, it's quite straightforward. The guides online are simple, follow the guide, and you've got a system that works. There could possibly be more around improving the performance, and maybe some more up-to-date calculators on sizing because some of the sizing information we've seen previously are a few years out of date..”

Verified user

[Read full review](#) 

Head of Cyber Security & CTO at a tech services company with 51-200 employees

Customer Service and Support

“The support experience generally depends on the issue complexity, but the team was very responsive and their technical guidance was also very good and constant. I would rate the customer support around nine out of ten..”

Vikram Chakravarthy

Cyber Security Engineer II (Vulnerability & Threat Management) at FICO

[Read full review](#) 

“We are working in India, and sometimes it takes a while to receive a response from the support. However, the solutions they provide are can do them. Their support is good.

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

Verified user

Senior Marketing Specialist II at Harman International

[Read full review](#) 

“The support from the Graylog community is helpful, but they can do better. The enterprise support doesn't really cater to open-source solutions. They only support you if you are an enterprise working on a POC. If you want to do a POC for an enterprise solution, they need assurances that you'll buy their enterprise solution. .”

CharlesNetshivhera

Senior DevOps Engineer at a financial services firm with 10,001+ employees

[Read full review](#) 

“Regarding technical support for Graylog, I can't comment much because I've not had to use it. Even though we have the enterprise products, we've not needed to use technical support because we've been using Graylog for many years and can fix most problems ourselves. There are some sizing documents online, but they were a few years out of date when we looked a few months back..”

Verified user

Head of Cyber Security & CTO at a tech services company with 51-200 employees

[Read full review](#) 

“Until now, I have only used the open-source version. I haven't used Graylog Security or Enterprise, so I'm not sure if there is technical support for the open-source version.

Usually, if I have issues that require troubleshooting, I consult the Graylog Community. Sometimes there are solutions on the forum..”

Atassi Kalo

Security Analyst at Netsharqs cybersecurity GmbH

[Read full review](#) 

“We didn't have any issues that we needed to fix in Graylog. It just worked for us. We do use other open-source products and commercial products, and the commercial product support is not always fantastic. For Graylog, we could solve all the issues by searching over the internet and on Stack Overflow. With other products, such as Metabase, which is an open-source business intelligence tool that we use, because half of our company is made of software developers, they can write a patch. We did that a couple of times, but with Graylog specifically, we haven't had a need to introduce any patches. It was just tweaking the config..”

Andrey Mostovykh

Senior Data Architect at a non-tech company with 201-500 employees

[Read full review](#) 

Other Advice

“Graylog Enterprise is cost-effective, but when compared with Elasticsearch, it can be more costly. I chose a rating of nine out of ten because there is not much that I would change to make it a perfect ten for me. I suggest using Graylog Enterprise, as it really helps to maintain and use everything effectively, ensuring the sustainability and health of the pods. My overall review rating for Graylog Enterprise is nine out of ten..”

Verified user

Junior Dev Ops Engineer at a consultancy with 11-50 employees

[Read full review](#) 

“If others are looking into using Graylog Enterprise and have multiple log sources that they need to monitor and correlate, I would recommend Graylog Enterprise. It is a good product, allowing them to ingest all the logs into a single platform where they can search, triage, create rules, and monitor every alert.

“Graylog Enterprise is a good, secure SIEM platform with mature investigation capabilities that works best when integrated into multiple log sources. I rate this product an eight out of ten..”

Vikram Chakravarthy

Cyber Security Engineer II (Vulnerability & Threat Management) at FICO

[Read full review](#) 

“We are now working with Splunk and [Wazuh](#). We used Graylog Enterprise for log management. I did not utilize Graylog Enterprise's advanced search capabilities.

When we installed and used Graylog Enterprise, it was sufficient. If I were to give a mark, it would be around seven to eight, or perhaps 7.5. We only used Graylog Enterprise for log management, and for this, I did not use anything. All that I did was manually follow the logs, take them manually, and do some parsing to see them in a better way. I think for this open source product with limited features, for a middle-sized company, it would be around nine, or perhaps even ten. I would rate this review a 7.5 overall..”

NicolaeClornii

Security Officer at JSC "Moldtelecom" S.A.

[Read full review](#) 

“Graylog is a purpose-driven tool, so we don't really use it in our company. Rather, we usually deploy it for our clients. Some clients wanted it for managing logs for forensic analysis or compliance reasons, and some wanted it as a security option.

Some clients abandoned it. Even though it is customizable, it doesn't offer much functionality out of the box. It requires a fair amount of effort and expertise to function. Maybe if there were prebuilt dashboards or processing, like [Wazuh](#), it could be adopted on a higher scale.

Overall, my rating for this product is seven out of ten..”

Atassi Kalo

Security Analyst at Netsharqs cybersecurity GmbH

[Read full review](#) 

“I would say it depends on the scenario. If you have logs and want to have an easier setup, then Graylog Enterprise is the best choice. However, if you go towards a more complex architecture, then you could use other options such as ELK or

Splunk. Graylog Enterprise, as far as logging is concerned, in terms of a small-scale setup and ease of use, is the best choice to go with. My overall rating for Graylog Enterprise is 7 out of 10 because of its flexibility and lightweight nature.

“The advice I would give to others looking into using Graylog Enterprise is to ensure that the data they are collecting is actually in a proper format so that it can be viewed more clearly within Graylog Enterprise's interface, focusing on the formatting of the data..”

Verified user

Platform Engineering at a comms service provider with 1,001-5,000 employees

[Read full review](#) 

“My impression of the overall visibility of Graylog is good. In the past few years, as it's transitioning from just an open-source product into more of an enterprise solution, they're trying to grow into that area and do more in the API space. I think it will get better, particularly for orchestration pieces. That's probably its weaker area compared to some of the other products such as [Microsoft Sentinel](#) or Log Analytics, where they have more hooks into different products. I appreciate that Graylog is moving towards that, and it's quite simple to get it stood up quickly. We have used it during security incidents with customers, and we have spun up a separate Graylog instance to help them with ransomware type issues. Graylog has supported our compliance and security monitoring activities because, for one of our customers who falls under the NIST 2 regulation due to critical infrastructure, we heavily use it for that side. However, for the rest, we don't tend to use it for compliance really. A lot of that's handled separately, so it's not really an area we do much with Graylog at the moment, but it could be something that we could do more with in the future. Graylog is not assisting us with our AI-driven data analysis or any operations with AI at the moment, but it could be something that we could do in the future. Currently, about 10 people are using Graylog in our company. We have plans to use Graylog more in the future as we deploy more. We run a private cloud for different platforms, and our intention is to have all of those systems folding their events into Graylog. Overall, I would rate Graylog at about a seven or eight. The only downside is some of the integrations; if it had more integrations, it would be easier to work with other tools. Contextually, they're transitioning from an open-source background to a more enterprise-oriented space, which understandably takes time..”

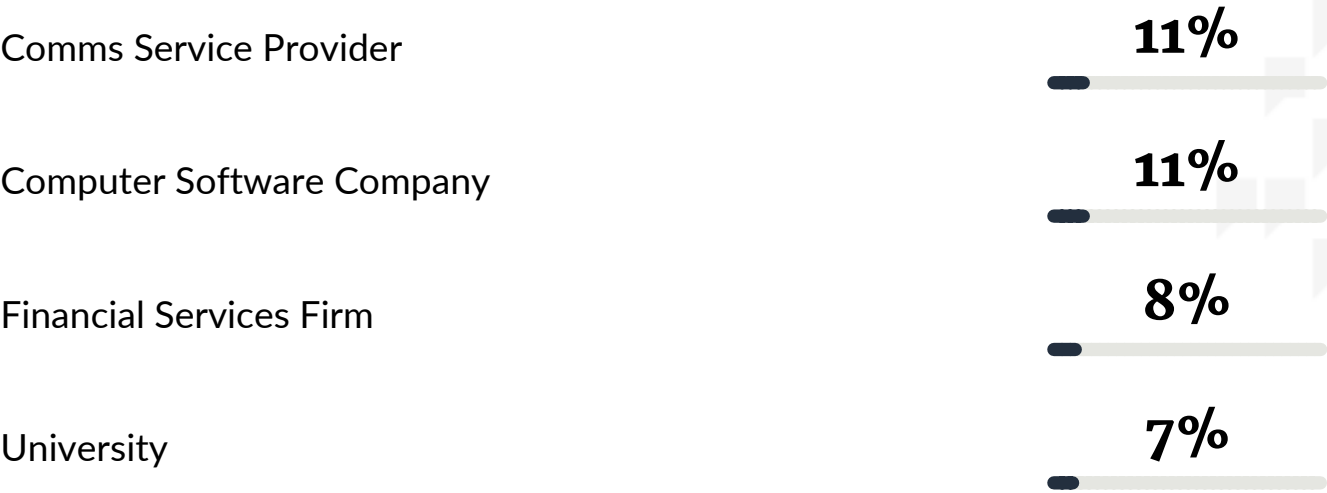
Verified user

Head of Cyber Security & CTO at a tech services company with 51-200 employees

[Read full review](#) 

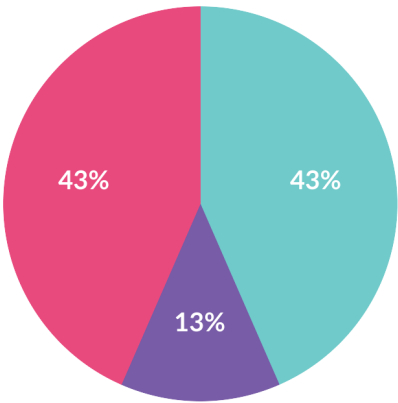
Top Industries

by visitors reading reviews

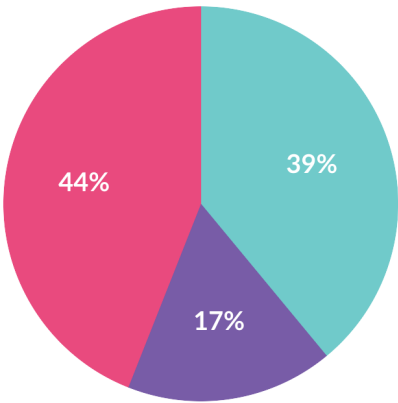


Company Size

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