aws marketplace

Graylog

Reviews, tips, and advice from real users






Powered by PeerSpot

Contents

Product Recap

Graylog

Graylog Recap

Graylog is purpose-built to deliver the best log collection, storage, enrichment, and analysis. Graylog is:

- Considerably faster analysis speeds.
- More robust and easier-to-use analysis platform.
- Simpler administration and infrastructure management.
- Lower cost than alternatives.
- Full-scale customer service.
- No expensive training or tool experts required.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- "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

- "Graylog is valuable because it bridges technical knowledge to non-technical teams, presenting complex backend processes in a simple timeline."

Ivan Kokalovic

DevOps Engineer at Proton Technologies

"The product is scalable. The solution is stable."

Nicolae Clornii

Security Officer at BC Energbank S.A.

"What I like about Graylog is that it's real-time and you have access to the raw data. So, you ingest it, and you have access to every message and every data item you ingest. You can then build analytics on top of that. You can look at the raw data, and you can do some volumetric estimations, such as how big traffic you have, how many messages of data of a type you have, etc."

Andrey Mostovykh

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

"Everything stands out as valuable, including the fact that I can quantify and qualify the logs, create pipelines and process the logs in any way I like, and create charts or data maps."

Peter Malaty

Sr. DevOps Engineer at TechStyle Fashion Group

"The best feature of Graylog is the Elasticsearch integration. We can integrate and we can run filters, such as an event of interest, and those logs we can send to any SIEM tool or as an analytic. Additionally, there are clear and well-documented implementation instructions on their website to follow if needed."

Lokesh Puthalapattu

Senior Marketing Specialist II at Harman International

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

Graylog is valuable because it bridges technical knowledge to non-technical teams, presenting complex backend processes in a simple timeline. It boosts the knowledge of sales and customer support teams by allowing them to see the backend operations without needing to read the code. Its API is flexible for visualization, and its powerful search engine efficiently handles large volumes of log data. Moreover, its stability, fast search capabilities, and compatibility with languages like ANSI SQL enhance its utility in IT infrastructure.

Ivan Kokalovic
DevOps Engineer at Proton Technologies

Read full review

"I like the correlation and the alerting. If I have multiple monitoring systems and I alert Graylog, Graylog will collect them and analyze them, and issue one alert.

We are only approximately four months into production and have not explored all of the features this solution offers. So far, it has everything we wanted.."

Verified user
Network Engineer at a media company with 10,001+ employees

Read full review

"Everything stands out as valuable, including the fact that I can quantify and qualify the logs, create pipelines and process the logs in any way I like, and create charts or data maps. One time, I created a geo map based on IP addresses accessing a website. The web server generates logs based on who's accessing the application, and we were able to extract the IPs from the logs and even create a chart on Graylog to map out exactly what countries the requests were coming from. Graylog is amazing. It's a beast.."

Peter Malaty
Sr. DevOps Engineer at TechStyle Fashion Group

Read full review

"One of the most valuable features is that you are able to do a very detailed search through the log messages in the overview. You are also able to attach a lot of details into your log messages.

When it came to integrating the solution with Java, it was quite easy. My colleagues used Graylog for some dashboards to show how many bugs there were per day or the overall performance of the applications. For the developers it's not super important, but it was quite a good way for the project manager to see that everything was all right.."

Jonas Leeb
Software Engineer & Co-Founder at Plexify 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

Other Solutions Considered

I evaluated Datadog among other solutions, but its pricing model deterred me since I preferred a solution like Graylog, which allowed testing without initial payment.

Ivan Kokalovic
DevOps Engineer at Proton Technologies

Read full review

I used my own logging service, Elasticsearch, and OpenSearch before transitioning to Graylog. OpenSearch was not as intuitive and had a steeper learning curve compared to Graylog.

Ivan Kokalovic
DevOps Engineer at Proton Technologies

Read full review

“We have tested IBM QRadar and now use it. First of all, the key factor is the pricing. I saw that IBM QRadar has an interactive dashboard, providing valuable insights to people. Additionally, I've seen that IBM QRadar has an agent that simplifies installations across various platforms without requiring intricate configurations. Also, IBM QRadar has automatic reporting..”

Nicolae Clornii
Security Officer at BC Energbank 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

"Before Graylog, we had a customer running IBM QRadar, which is a big security logging platform. We used other products such as RSyslog, Kiwi Syslog, which is Windows-based, and Syslog-ng, among others.The decision to switch to Graylog was influenced by my appreciation of its user interface. It separates out the ingestion from the backend. For instance, if Graylog is running and you take the backend down, you don't lose events. In contrast, with RSyslog, if you turn it off, you can't do backend-frontend maintenance, which is an advantage Graylog offers. It also handles clustering nicely, making it easy to scale up quickly.."

Verified user

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

Read full review

ROI

Real user quotes about their ROI:

"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 have one SIEM tool to integrate the log source for other containers and user-related logs. Those logs were integrated into Graylog. When required those logs Graylog gets sent to a SIEM tool. ."

Lokesh Puthalapattu
Senior Marketing Specialist II at Harman International

Read full review

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

Read full review

"We had two use cases. In the beginning, log centralization was the main thing, and this was the most frequent use of Graylog, but we also tried to use it for analytics. Graylog was maintained by the data lake team, and we were looking for tools that were suitable for analytics. We felt that Graylog looks real-time. It had some graphs and dashboards. So, we had an idea to use it for analytics. ."

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

Read full review

In my opinion, the best use case for Graylog is for backend services due to its excellent real-time updates. It is especially effective with strong type languages, like Java or C++. The streaming of messages happens with the GELF protocol over UDP, making it quite fast. Deploying Graylog into a Docker image where microservices are placed allows for easy log retrieval. Logs from different Docker machines can be combined into one Graylog instance, providing a complete view of backend behavior for both developers and customer support teams.

Ivan Kokalovic
DevOps Engineer at Proton Technologies

Read full review

"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
Security Analyst at Netsharqs cybersecurity GmbH

Read full review

“I have my own recipe for an infrastructure code where I integrate Fluent Bit with Kubernetes. It scrapes the logs off of all the member nodes of Kubernetes and then it chips that to an input on Graylog. That way, when developers want to troubleshoot an application but don't want to use anything Kubernetes CLI-related, they can jump straight to Graylog. They can type the name and the type of deployment that they're looking for and get all of the logs pulled into one place. Essentially I use this solution to give developers a way to look at all the logs in an aggregated form. It's very helpful.

I also use the solution to extract and quantify data and metrics from the logs. For example, let's say you're running the wallet application and you want to make sure that you are getting the minimum 404's when somebody is trying to make a payment. You can essentially extract the code on Graylog and it will give you a really nice view of how often your wallet times out, or overall performance. If you're looking specifically from a security standpoint, if the application is seeing something that should not be seen, you have a way to log that.

I also use it for building charts and live logging. Also, the pipelines allow you to take a raw log, create something out of it, and transform it into something else, so I use that for streams, presentations, metrics, and health checks from an app runtime standpoint..”

Peter Malaty
Sr. DevOps Engineer at TechStyle Fashion Group

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.

The initial setup of Graylog was straightforward, provided the codebase was prepared for logging. The documentation, although not visually appealing, was informative and helpful.

Ivan Kokalovic

DevOps Engineer at Proton Technologies

Read full review

"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

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

Read full review

"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

Sr. DevOps Engineer at TechStyle Fashion Group

Read full review

"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

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

Read full review

Customer Service and Support

“The technical support is a weak point in this product. It's not so easy to contact them and they don't answer immediately. Sometimes it takes a lot of time and the wait is difficult. If I had enough documentation I might not need the support. .”

Verified user
Entrepreneur at a tech services company with 51-200 employees

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..”

Lokesh Puthalapattu
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

I would recommend Graylog for its stability, API capabilities, and fast search engine. However, it's not ideal for developers lacking in setting up comprehensive logging in their codebase. I rate Graylog an eight out of ten.

Ivan Kokalovic
DevOps Engineer at Proton Technologies

Read full review

“The solution's community version works well for a lesser workload. It will help if you opt for the solution's enterprise version if you plan to increase the load.

I recommend the solution to others and rate it as a seven..”

Shivam-Tiwari
DevOps Engineer Intern at MyKaarma

Read full review

"My advice to people considering this solution is to first determine where they can use it. The server sizing depends on the amount of logs generated and where you get the logs from. For example, it it a Kubernetes cluster with a lot of things on it, or just a bunch of VMs, or just a couple of VMs? What's the size of that? Based off of this, you would then decide the server sizing and how big your Elasticsearch needs to be and how scalable it needs to be. Graylog is like ELK Stack. It's very, very resource hungry.

I would rate this solution as a seven out of ten. ."

Peter Malaty
Sr. DevOps Engineer at TechStyle Fashion Group

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'm pretty happy with the features of the product, but I'm not happy with the infrastructure costs. Feature-wise or from the end user perspective, Graylog is just great.

For small enterprises, it's a good start because they tend to use cheaper products, at least until they grow. Graylog is a good fit there because you can pick a very cheap cloud provider and then just install it there. It is pretty cheap. For big companies that are focused on reliability and availability, Graylog either requires over-provisioning or will cost a lot, which is not ideal. There are better solutions out there in the market, but one important point is that Graylog can be placed in your local data center. Some companies are very suspicious of clouds or have some restrictions from authorities or as per their policies and business model. T here are countries, for example, Pakistan, where the network is poor, and if you use the closest data center of any cloud provider, that will most likely be Thailand. For these types of setups, Graylog is pretty much the only choice.

Before Humio, I would have rated it a 10 out of 10. It's a great product, but because of its cost, I would rate it a 9 out of 10. .”

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

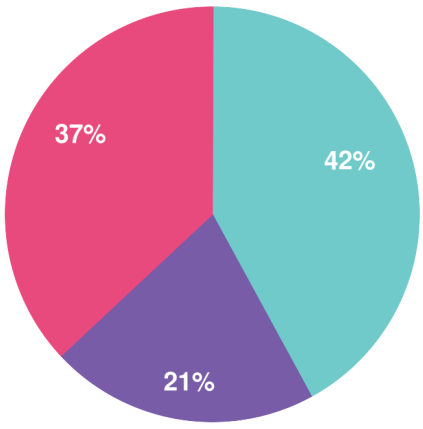
Top Industries

by visitors reading reviews

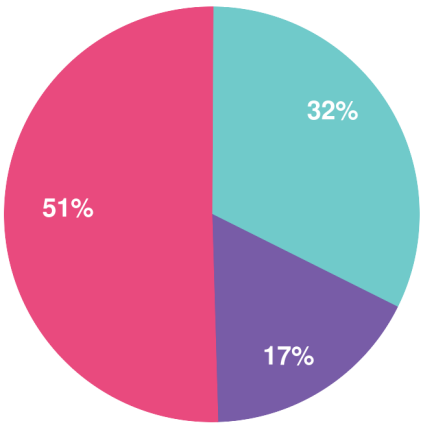
Computer Software Company	17%
Comms Service Provider	11%
Government	8%
University	7%

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 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