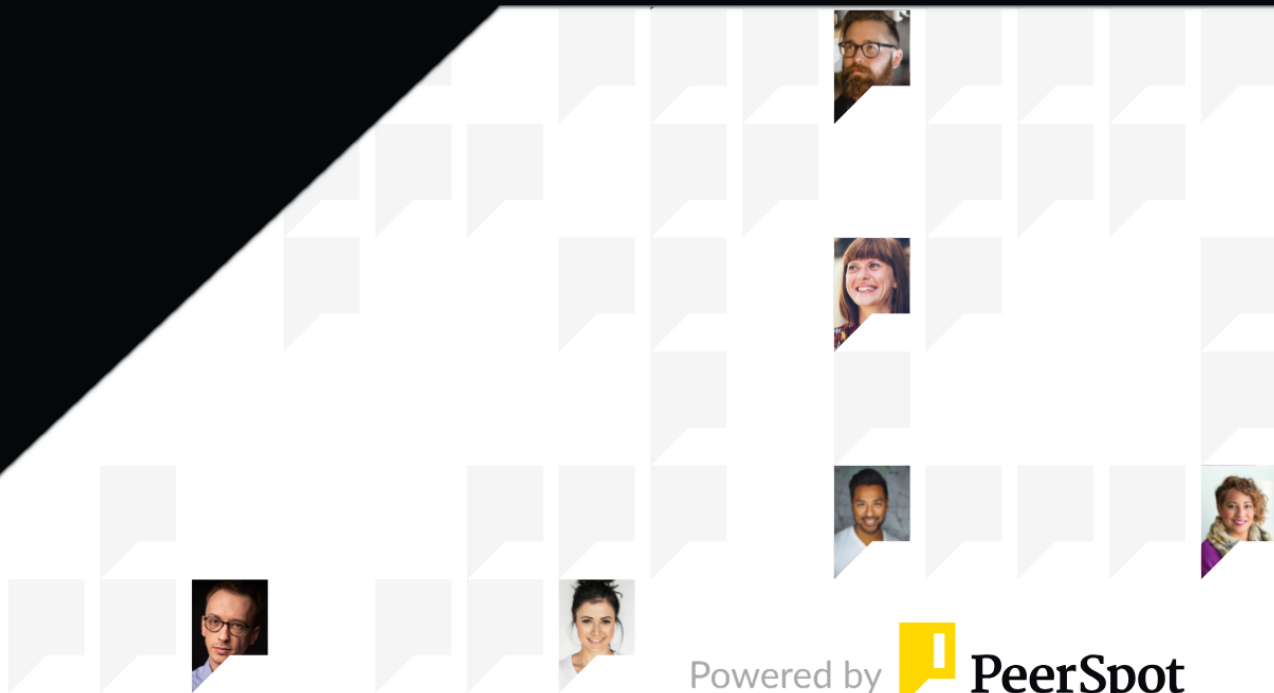


aws marketplace

rsyslog server

Reviews, tips, and advice from real users



Powered by  **PeerSpot**

Contents

Product Recap..... 3 - 4

Valuable Features..... 5 - 10

Other Solutions Considered..... 11 - 12

ROI..... 13 - 14

Use Case..... 15 - 17

Setup..... 18 - 19

Customer Service and Support..... 20

Other Advice..... 21 - 24

Trends..... 25 - 26

About PeerSpot..... 27 - 28

Product Recap



rsyslog server

rsyslog server Recap

Rsyslog server is a robust and versatile tool used for forwarding log messages in an IT environment. It supports various protocols and can handle high data volumes with speed and efficiency.

Rsyslog server is known for its modular design that allows easy integration in complex IT networks. It can transmit logs from many sources, ensuring no data loss even in high-load scenarios. Its compatibility with various formats makes it adaptable to different IT infrastructures, offering a reliable solution for log management and monitoring. Advanced features like message queuing and customizable output formats enhance its functionality for IT administrators.

What are some key features of rsyslog server?

- **Protocol Support:** Handles Syslog, HTTP, and various other protocols for log forwarding.
- **Modular Design:** Offers flexibility for integration into different network architectures.
- **High-Performance:** Can process massive volumes of log data with minimal latency.
- **Message Queuing:** Ensures smooth handling of incoming data, preventing loss during peaks.
- **Customizable Outputs:** Supports various output formats to suit different needs.

What benefits and ROI can users expect in reviews?

- **Efficiency:** Optimizes log management processes, saving time for IT teams.
- **Scalability:** Grows with expanding IT infrastructure without compromising performance.
- **Reliability:** Provides consistent performance, ensuring logs are processed accurately.
- **Cost-effectiveness:** Reduces the need for multiple tools by offering comprehensive features.
- **Adaptability:** Fits into existing IT setups, minimizing disruption and transition costs.

Rsyslog server is implemented across multiple industries for enhancing IT operations. In finance, it's used for secure log management and compliance tracking. In healthcare, it ensures data integrity and confidentiality through efficient log processing. Manufacturing sectors utilize it for monitoring and improving operational efficiency by analyzing machine logs in real time.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- ✓ “Rsyslog server's AI capabilities depict it as a data pipeline feeding AI systems, working hand in hand with AI for anomaly detection, ops automation, and log analysis through the collected syslog data.”



Esther Sultaana

Storage Consultant Storage at Hewlett Packard Enterprise

- ✓ “The best feature rsyslog server offers is syslog recording, serving as the main and most important feature by recording syslogs and receiving them from TCP or UDP, other UDP servers, and forwarding those logs to even other servers, allowing for daily syslog handling in any direction, TCP, UDP, local, or remote.”



Ms Ms

Founder at ONE Energy-IT GmbH

- ✓ “These features make my day-to-day work easier and more efficient because whenever I find any failure or boot problems in a client machine, I can easily identify the issue.”



Siddesha Nc

Assistant System Admin at a computer software company with 51-200 employees



“The easy configuration and quick monitoring of rsyslog server help me in my day-to-day work as it saves my time and makes my troubleshooting easier.”



Verified user

ITA at a tech vendor with 10,001+ employees



“The impact of rsyslog server on my organization has been positive, making processes easier, faster, and more reliable, as before its integration with the firewall, we lacked insight into policies governing incoming and outgoing traffic.”



Baljindra Singh

IT System Administrator at a tech company with 201-500 employees

What users had to say about valuable features:

“The best feature of rsyslog server is easy configuration, which includes straightforward setup and quick monitoring of the logs.

“The easy configuration and quick monitoring of rsyslog server help me in my day-to-day work as it saves my time and makes my troubleshooting easier. Once I configure the details in rsyslog.conf and restart rsyslog server, I can quickly access the information, which is very useful for troubleshooting purposes..”

Verified user

[Read full review](#) 

ITA at a tech vendor with 10,001+ employees

“The best features of rsyslog server are its support for both UDP and TCP log ingestion, flexible log routing, self-hosting capability, log rotation management, and reliable buffering and forwarding features.

These capabilities are essential in our environment because our firewalls generate a large volume of logs every day. Proper log rotation prevents files from becoming too large and difficult to analyze during investigations.

Another major advantage is the ability to offload buffering, retries, forwarding, and parsing from the firewall itself. This reduces firewall workload while ensuring logs are securely stored and available for future analysis..”

Baljindra Singh

[Read full review](#) 

IT System Administrator at a tech company with 201-500 employees

“The best feature rsyslog server offers is syslog recording. What I appreciate about the syslog recording feature is that it serves as the main and most important feature, recording syslogs and receiving syslogs from TCP or UDP, other UDP servers, and forwarding those logs to even other servers, allowing for daily syslog handling in any direction, TCP, UDP, local, or remote.

rsyslog server has had the usual impact on my organization; it does not matter to me if it is rsyslog server or another syslog server; it is just my preference, and I do not have specific reasons why it became this preference. There has been just personal preference in noticeable differences in reliability, performance, or troubleshooting since I have used rsyslog server compared to others..”

Ms Ms

Founder at ONE Energy-IT GmbH

[Read full review](#) 

“In my opinion, the best features rsyslog server offers include the ability to send enormous logs from client OS to server devices, which I can fix with scripts. I can easily identify the host machine and what kind of logs it contains, whether it is an application log or operation log, and it sorts them based on how I write the script, allowing it to redirect and resend the logs.

These features make my day-to-day work easier and more efficient because whenever I find any failure or boot problems in a client machine, I can easily identify the issue. I can go to the log machine and check what kind of problem it is, whether it is a web server crash or a main server crash, and based on the logs and messages, I can easily identify and troubleshoot the issues. Furthermore, I can monitor and audit the logs as well, including SSH logins, and track who last logged in and who is currently logged in on the machines, as well as easily track any failed login attempts in case of suspicious activities.

rsyslog server has positively impacted my organization by providing centralized logging for our machines. I implemented it for the servers, database, application servers, and some network devices as well. I get day-to-day logs, which I can monitor easily and audit those devices, impacting our day-to-day productivity..”

Siddesha Nc

[Read full review](#) 

Assistant System Admin at a computer software company with 51-200 employees

“The best features that rsyslog server offers include the ability to filter, tag, and rewrite logs, with logs stored in databases and files, then forwarded to various destinations such as SIEM or files as needed. Of course, the client sends the logs.

“Out of those features, I find myself relying most heavily on the logging capabilities it pulls from everything that is connected to Unix or Linux boxes, allowing me to see any particular issues or errors that may be occurring. The logs are stored in files or databases and they can be forwarded to me, even emailed directly.

“rsyslog server has positively impacted my organization, particularly with disaster recovery logging, where alerts for failures allow me to see failover events and any replication issues, especially within managed healthcare environments. It can indeed be used for HIPAA, pulling data from the entire infrastructure including Unix and Linux servers, network devices, firewalls, and storage arrays.

“Regarding how rsyslog server has improved efficiency and compliance, it provides insight into what's happening within the infrastructure as a high-performance systems log daemon receiving logs from the entirety of the network through UDP and TCP, writing to files, databases, or SIEM systems. It's user-friendly for Unix and Linux admins or engineers because it's been familiar for so long, and it certainly is not outdated..”

Esther Sultaana

Storage Consultant Storage at Hewlett Packard Enterprise

[Read full review](#) 

Other Solutions Considered

“I did not use another centralized logging solution before rsyslog server. We implemented it based on organizational requirements, and it has proven to be reliable and highly effective for our environment..”

Baljindra Singh

IT System Administrator at a tech company with 201-500 employees

[Read full review](#) 

“Before choosing rsyslog server, we evaluated Datadog. However, we preferred rsyslog because it provided a cost-effective and flexible self-hosted solution for centralized log collection and investigation without depending heavily on third-party licensing costs..”

Baljindra Singh

IT System Administrator at a tech company with 201-500 employees

[Read full review](#) 

“Before choosing rsyslog server, I evaluated options such as Splunk and some SIEM tools such as Graylog or IBM QRadar, but those were licensed. I cannot use them without going through enterprise purchases, which are financially prohibitive..”

Siddesha Nc

Assistant System Admin at a computer software company with 51-200 employees

[Read full review](#) 

ROI

Real user quotes about their ROI:

“I have seen zero return on investment with rsyslog server as it is an open-source tool. I just download it and do scripting for the kind of logs I want, and it is very easy to configure without any associated costs..”

Siddesha Nc

[Read full review](#) 

Assistant System Admin at a computer software company with 51-200 employees

“I have seen a return on investment by making use of syslogs, which helps predict anomalies in server environments and storage systems. For instance, alerts from tools such as Pure or Dell EMC, and reporting replication issues from Zerto or similar applications, always provide immediate notifications that are essential for IT operations..”

Esther Sultaana

[Read full review](#) 

Storage Consultant Storage at Hewlett Packard Enterprise

“The initial setup was straightforward. We configured the firewall devices to forward web filtering, DNS filtering, and application filtering logs to the rsyslog server.

On the rsyslog side, we created separate log collection files and automated daily log rotation with compression of older logs for future investigations and retention management..”

Baljindra Singh

IT System Administrator at a tech company with 201-500 employees

[Read full review](#) 

Use Case

“My main use case for rsyslog server is syslogging. A quick, specific example of how I use it for logging is collecting any syslog from a Unix server, including syslogs from firewalls and routers..”

Ms Ms

Founder at ONE Energy-IT GmbH

[Read full review](#) 

“My main use case for rsyslog server is resending logs to my log server from other servers, and I am redirecting logs from regular servers to one log server.

For resending logs using rsyslog server, I configure one server and enable it on the Ubuntu machine to which I redirect all servers' logs. I enable UDP and TCP for the logs in a firewall, and then on end machines such as servers, I go to rsyslog and enable it. After that, I configure the IPs from the client machine, meaning the server machine, to rsyslog server.

I use rsyslog server exclusively for this purpose..”

Siddesha Nc

Assistant System Admin at a computer software company with 51-200 employees

[Read full review](#) 

“Our primary use case for rsyslog server is centralized log collection, long-term retention, and security monitoring. We also use it as an intermediate logging layer before forwarding logs to our CrowdStrike Falcon cloud platform for XDR and MDR analysis.

We built an automated pipeline where firewall devices send logs to rsyslog server, which then processes, stores, and forwards the logs to CrowdStrike Falcon. This helps us detect abnormal firewall activity, suspicious traffic, and security-related events in near real time.

The solution is also valuable for historical investigations because it allows us to retain logs locally for root cause analysis and back-dated event reviews..”

Baljindra Singh

IT System Administrator at a tech company with 201-500 employees

[Read full review](#) 

“My main use case for rsyslog server is that it's a logging system for Unix and Linux that collects, stores, and filters logs from various devices, which means I'm working with infrastructure, VMware, and security, something that has been around ever since Unix was established. I pull system logs to see what's going on in systems around the Unix environment and outside of it.

“A quick specific example of how I use rsyslog server in my daily work is through centralized logging, where it collects data from Linux servers, Unix servers such as Solaris and AIX, network devices, firewalls, storage arrays, and VMware hosts, pulling logs from everything the Unix and Linux hosts are connected to. These days, it's also used considerably with security, similar to Splunk or Azure Sentinel, and definitely for compliance and audit retention for HIPAA and disaster recovery logs.

“I have additional information about my main use case regarding how I use rsyslog server day to day, especially with disaster recovery, as I can track failover events and replication issues when working with tools such as Zerto, addressing kernel issues specifically related to the Unix and Linux servers themselves.

“rsyslog server is commonly used for many things in my work, including disaster recovery event tracking, storage arrays such as Dell EMC, NetApp, Pure, and security compliance logging, as well as VMware ESXi host logging..”

Esther Sultaana

Storage Consultant Storage at Hewlett Packard Enterprise

[Read full review](#) 

Setup

The setup process involves configuring and preparing the product or service for use, which may include tasks such as installation, account creation, initial configuration, and troubleshooting any issues that may arise. Below you can find real user quotes about the setup process.

“I have always looked at system logs within Unix and Linux because they come integrated with the OS, offering stability that makes it a default solution, even if other tools were available. Setting up a dedicated rsyslog server enhances that efficiency further..”

Esther Sultaana

[Read full review](#) 

Storage Consultant Storage at Hewlett Packard Enterprise

“I manually configured the rsyslog.conf on a server, and there is no licensing for rsyslog server. Splunk, in contrast, uses licensing based on daily data ingestion volume, which relates to the indexing count of the logs in Splunk..”

Verified user

[Read full review](#) 

ITA at a tech vendor with 10,001+ employees

“I did not purchase rsyslog server through the AWS Marketplace. My experience with pricing, setup cost, and licensing is that I have never licensed rsyslog server, as it is open source, so the question does not make sense..”

Ms Ms

[Read full review](#) 

Founder at ONE Energy-IT GmbH

“The initial setup was straightforward in our environment. We configured the firewall devices to forward web filtering, DNS filtering, and application filtering logs to the rsyslog server using the server’s IP address for centralized log ingestion.

On the rsyslog side, we created separate log collection files and routing rules so that firewall logs are stored independently for easier analysis and troubleshooting. We also implemented automated daily log rotation and compression of older log files for long-term retention and future forensic investigations..”

Baljindra Singh

[Read full review](#) 

IT System Administrator at a tech company with 201-500 employees

Customer Service and Support

“Customer support largely depends on the Unix or Linux server provider; for example, Red Hat has notable support, and HP or IBM also offer reliable help..”

Esther Sultaana

Storage Consultant Storage at Hewlett Packard Enterprise

[Read full review](#) 

“Customer support for rsyslog server has not been needed since I maintain everything myself. If anything happens, I am responsible for finding and fixing the issues; therefore, there is no need to reach out for customer service..”

Siddesha Nc

Assistant System Admin at a computer software company with 51-200 employees

[Read full review](#) 

Other Advice

“My advice for others looking into using rsyslog server is that it is easy to use and configure. Once the network device parameters are configured in rsyslog.conf, I can easily monitor the log files, which are useful for troubleshooting purposes. I would rate this product a 9 out of 10..”

Verified user

ITA at a tech vendor with 10,001+ employees

[Read full review](#) 

“I would rate rsyslog server 10 out of 10 for centralized logging, log forwarding, and long-term forensic analysis.

For organizations considering rsyslog server, I highly recommend it because it is stable, scalable, lightweight, and highly effective for firewall and infrastructure log management..”

Baljindra Singh

IT System Administrator at a tech company with 201-500 employees

[Read full review](#) 

“That is all for me regarding features, flexibility, or ease of use. I rate rsyslog server an eight on a scale of one to ten because I am mostly happy, but sometimes it does not work immediately, and I have to work with the logs to figure out what is happening. Regarding rsyslog server's AI capabilities, I think about its governance and security. I do not care for AI in rsyslog server ensuring its accuracy and reliability of output. I have no specific advice for others looking into using rsyslog server other than to follow the usual Google setup and be happy. .”

Ms Ms

Founder at ONE Energy-IT GmbH

[Read full review](#) 

“I can share specific outcomes regarding rsyslog server, as it has saved me time and improved my ability to respond to issues. Recently, I encountered a problem where my SSH server was down automatically, which caused some users to be unable to log in. From that log, I checked and found critical bugs in SSH, allowing me to troubleshoot the issue within a short amount of time.

My advice for others looking into using rsyslog server is that if someone wants to set up a local environment with a budget-friendly approach, they should choose rsyslog server. If they have ten to fifteen machines in their cloud or private cloud, they can use rsyslog server without issues, making it easier to improve their daily productivity. I would rate this product nine out of ten..”

Siddesha Nc

Assistant System Admin at a computer software company with 51-200 employees

[Read full review](#) 

“I give rsyslog server a rating of ten out of ten. The reason is that long before we

focused so heavily on cloud technologies, the Unix world had a robust system to look into the logs, revealing what's going on within those servers and databases. My experience with Unix systems shows that most Unix or Linux servers contain databases, marking it as an absolute ten in functionality; it's as relevant today as it ever was.

“rsyslog server's AI capabilities depict it as a data pipeline feeding AI systems, working hand in hand with AI for anomaly detection, ops automation, and log analysis through the collected syslog data. This allows for AI model analysis of logs, detecting unusual patterns, suspicious firewall events, and potential disaster recovery replication anomalies or storage errors predicting failure. There is immense potential in processing those rsyslog events filtered through AI.

“The accuracy of rsyslog server's output is very high, as is its reliability. This is due to its ability to pull crucial data from infrastructure and connected servers. When using AI-driven anomaly detection tools such as [Azure Sentinel](#) or Splunk's toolkit, I can pinpoint a variety of issues from replication lag and network anomalies to VMware host instability, maintaining a high level of stability and reliability through my use.

“The fact that rsyslog server can pull from the entire infrastructure speaks volumes for its capabilities. Being a part of the Unix and Linux OS, I can easily log in and examine syslog logs, piping data to the screen or receiving it via email to monitor server activities. In terms of improvements, it has been extended to analyze Azure Sentinel pipelines or firewall logs, enhancing security compliance through a comprehensive look at various systems' logs.

“I would advise others considering rsyslog server to realize that those who have Unix or Linux systems are already using it, as introducing AI utilization to pipe our syslogs offers significant operational advantages. It undeniably simplifies processes across IT.

“To summarize my additional thoughts about rsyslog server, it acts as a centralized logging system utilized within Unix and Linux environments, collecting, filtering, and forwarding logs from multiple devices including storage, VMware, and cloud security for disaster recovery. Using AI enhances its functionality, allowing for smarter log filtering and management. My overall

review rating for rsyslog server is ten out of ten..”

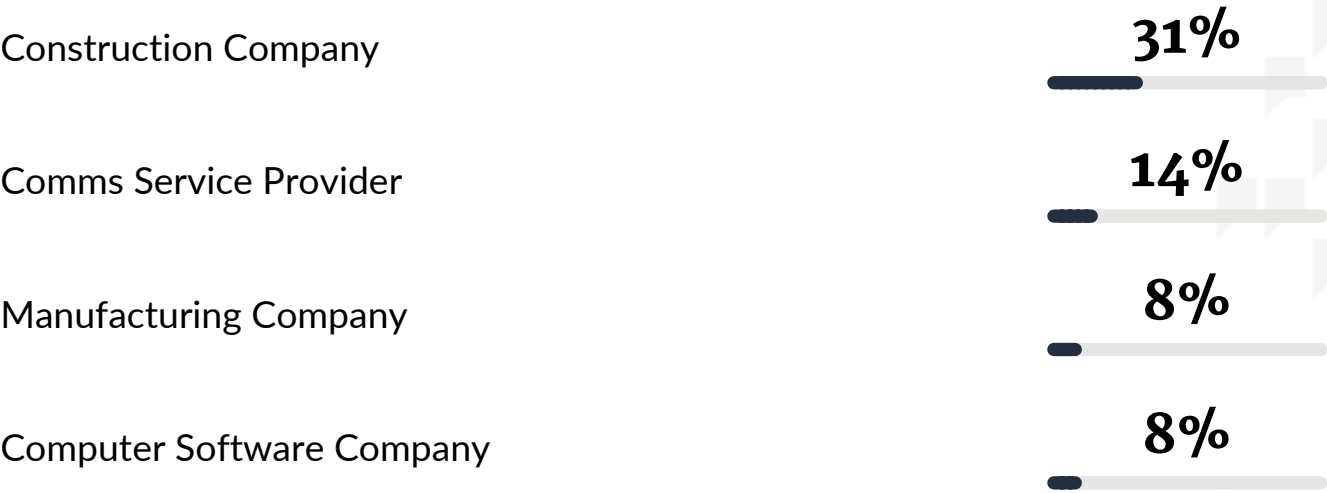
Esther Sultaana

Storage Consultant Storage at Hewlett Packard Enterprise

[Read full review](#) 

Top Industries

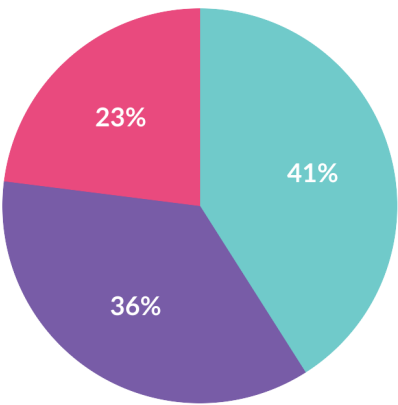
by visitors reading reviews



Company Size

by reviewers

by visitors reading reviews



Large Enterprise Midsized Enterprise Small Business

About this buyer's guide

Thanks for downloading this PeerSpot report.

The summaries, overviews and recaps in this report are all based on real user feedback and reviews collected by PeerSpot's team. Every reviewer on PeerSpot has been authenticated with our triple authentication process. This is done to ensure that every review provided is an unbiased review from a real user.

Get a custom version of this report... Personalized for you!

Please note that this is a generic report based on reviews and opinions from the collective PeerSpot community. We offer a [customized report](#) of solutions recommended for you based on:

- Your industry
- Company size
- Which solutions you're already considering

The customized report will include recommendations for you based on what other people like you are using and researching.

Answer a few questions in our short wizard to get your customized report.

[Get your personalized report here](#)

About PeerSpot

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

PeerSpot helps tech professionals by providing:

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

Use PeerSpot to:

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

Join PeerSpot to connect with peers to help you:

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

Visit PeerSpot: www.peerspot.com

PeerSpot

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

reports@peerspot.com

+1 646.328.1944