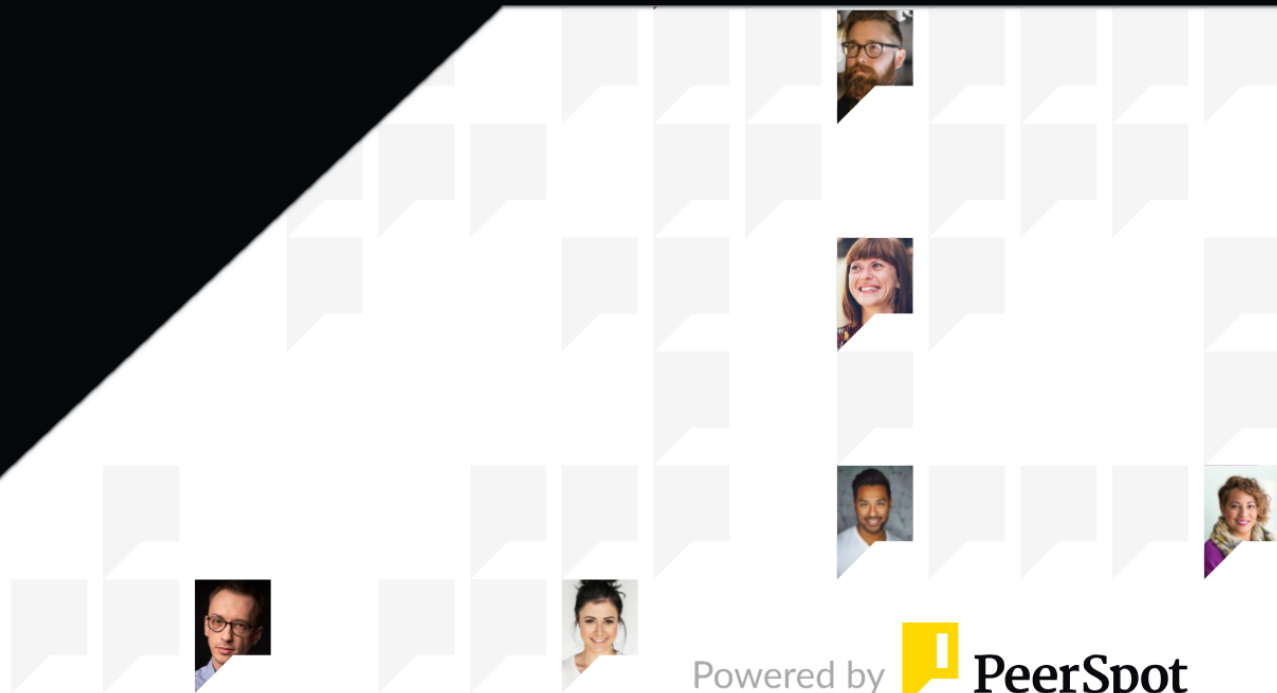




Splunk Enterprise Platform

Reviews, tips, and advice from real users



Powered by  **PeerSpot**

Contents

Product Recap..... 3 - 4

Valuable Features..... 5 - 12

Other Solutions Considered..... 13 - 14

ROI..... 15 - 17

Use Case..... 18 - 21

Setup..... 22 - 24

Customer Service and Support..... 25 - 26

Other Advice..... 27 - 30

Trends..... 31 - 32

About PeerSpot..... 33 - 34

Product Recap



Splunk Enterprise Platform

Splunk Enterprise Platform Recap

Splunk Enterprise Platform provides high flexibility and integration, featuring strong analytics, data ingestion, and real-time monitoring, catering to diverse industry needs and enhancing threat detection and data analysis.

Splunk Enterprise Platform is renowned for its powerful capabilities in log management, threat detection, and data visualization. It supports infrastructure monitoring and anomaly detection, crucial for Security Incident and Event Management operations. With its scalable architecture, users can efficiently manage data ingestion and create personalized dashboards, utilizing Splunk Processing Language for comprehensive querying and system performance assessment. This platform offers enhanced threat detection through its robust anomaly detection features and real-time monitoring capabilities, with machine learning enabling predictive analytics.

What features make Splunk Enterprise Platform stand out?

- **Powerful Analytics:** Offers Splunk Processing Language for complex data querying.
- **Data Ingestion:** Facilitates seamless data capture from multiple sources.
- **Customizable Dashboards:** Allows user-defined views for better decision-making.
- **Anomaly Detection:** Provides robust tools for identifying unusual patterns.
- **Real-time Monitoring:** Enables tracking of system activities as they occur.

What benefits do users gain when evaluating Splunk Enterprise Platform?

- **Scalable Architecture:** Adapts to growing data needs efficiently.
- **Enhanced Threat Detection:** Improves security management processes.
- **User-friendly Interface:** Simplifies navigation and usage.
- **Seamless Integration:** Works with other tools to streamline operations.
- **Efficient Log Management:** Organizes vast data quantities effectively.

In industries like finance, healthcare, and technology, Splunk Enterprise Platform is implemented to monitor infrastructure, manage logs, and enhance security protocols. Companies utilize its predictive analytics for strategic planning and operational efficiency, focusing on integration with AWS, EDR, and firewalls for comprehensive data visualization and threat management.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- ✓ “Splunk Enterprise Platform has had some of the biggest positive impacts on our organization, including improvements in incident response time, faster threat detection, increased efficiency by consolidating tools, and automated compliance reporting that saves hours of manual work and improves audit readiness.”



Koyena Paul

Managed Security Services Associate at Accenture

- ✓ “The governance tools provided by Splunk Enterprise Platform are very good, and it is a very good platform that provides you with a way to maintain data security.”



Sama Parveen

Cloud Technology Support Senior Analyst at a tech vendor with 10,001+ employees



“I assess the effectiveness of Splunk Enterprise Platform in detecting anomalies and preventing system outages as very strong; for over two to three decades, it has provided centralized log visibility, real-time monitoring, and analytics correlation, which is robust for threat detection and incident investigation.”



Vikas Pandita

Global Head Of Security Architecture Digital & Technology at Aramex



“In my opinion, the best features Splunk Enterprise Platform offers are its flexibility and ability to accomplish a variety of different things depending on the requirement.”



Will Searle

Director, Consultant



“Splunk Enterprise Platform has a vast and versatile powerful search engine with which I can handle all queries, and creating use cases and the search and dashboard is the main selling point, allowing me to visualize live dashboards.”



FaisalKhan5

SOC A2 at Innodata-ISOGEN

- ✓ “Since the implementation of Splunk, we have significantly reduced our TCO in maintaining data and collecting logs.”



Verified user

Splunk Engineer at a consultancy with 11-50 employees

- ✓ “Overall, the feature set of Splunk Enterprise Platform is comprehensive and flexible.”



Mahendra Rathal

Fine at PCS Solutions

What users had to say about valuable features:

The best features for me include recently starting to mess with creating bar charts and pie charts within Splunk Enterprise Platform console versus exporting the data and then doing it in Excel. That has been very beneficial to me, having a one-stop shop for things of that nature.

It has given us, from an engineering perspective, the ability and the scalability to move at haste when it is time to investigate different alerts that we need to triage. Things that may be false positive or true positive, we are able to delineate really fast, and also gather important data for those C-suite folks who may need the type of data to support KPIs and things of that nature. .”

Verified user

cloud security engineer at a tech vendor with 11-50 employees

[Read full review](#) 

“The best feature Splunk Enterprise Platform offers is usability.

What specifically stands out to me about usability is the dashboards and alert setup.

Splunk Enterprise Platform has positively impacted my organization by allowing us to respond quickly to servers being offline or having resources consumed too heavily.

I have seen improvements in both response time and avoiding outages because of Splunk Enterprise Platform. Splunk Enterprise Platform is stable and seems to be pretty scalable. Customer support for Splunk Enterprise Platform is fairly good..”

Kyle Jarius

Cloud Engineer at a construction company with 1,001-5,000 employees

[Read full review](#) 

“The best features Splunk Enterprise Platform offers include alerting.

What I appreciate most about Splunk Enterprise Platform's alerting features is that it notifies me of something bad that is about to happen before it happens.

Alerting is the main highlight for me regarding features.

Splunk Enterprise Platform has positively impacted my organization, as we are ahead of the curve in terms of when we discover issues.

Being ahead of the curve has helped by saving time..”

Verified user

software engineer at a government with 51-200 employees

[Read full review](#) 

“The best features Splunk Enterprise Platform offers include a robust environment and platform for all the various devices on the network, an easy ability to update, a great support team from Splunk, which helps us stay on track and expand our functionality, and an ecosystem with so many options to improve visibility of durability and everything else.

“The feature I rely on the most or find the most valuable in my day-to-day work is the ability to keep eyes and ears on our network and be able to search for any events that need attention and make sure the network and all the devices are online.

“Splunk Enterprise Platform positively impacts my organization by helping us keep all of our devices online and healthy and helped us prove we meet the requirements for the CCRI audit..”

Carlos Ciscoor

IT systems engineer at a outsourcing company with 5,001-10,000 employees

[Read full review](#) 

“Splunk Enterprise Platform offers great observability into all my apps, as well as being able to use the GUI to edit different things and be able to provide the best experience for our internal teams so that way we can provide the best experience for our customers.

“The overall visibility of Splunk Enterprise Platform is great, but I do really appreciate being able to do specific searches for different teams if they're missing data or if they need extra data in, as well as looking at dashboards and enabling those teams to have the most efficient and productive time.

“I think it handles large data very well. It seems to regulate and maintain itself very well. It corrects itself back on course to resolve those errors..”

Verified user

[Read full review](#) 

IT Monitoring Analyst at a insurance company with 5,001-10,000 employees

“Splunk Enterprise Platform is very user-friendly, and our users love the ability to use the search interface, which helps determine issues when you know something is happening, but you do not know where it is happening in all of our various items that exist, all the systems that produce logging data.

For our use case, the absolute best feature of Splunk Enterprise Platform is that you can get data into Splunk Enterprise Platform from anywhere, and that is really useful because there are just so many different sources.

We are primarily using Universal Forwarders, but we also use HEC forwarders and heavy forwarders to integrate different data sources.

Our users definitely love the ability to create their own dashboards in Splunk Enterprise Platform so that they can monitor the applications that they are involved in, making that a popular feature.

Splunk Enterprise Platform has made it a lot faster to find problems. This is very much Splunk Enterprise Platform's core functionality where instead of having to go and SSH into different servers and look at log files on each one, which can take a lot of time, you are able to search via the GUI and pull up logs across all of the applications being monitored..”

Verified user

[Read full review](#) 

Application Server Administrator at a healthcare company with 10,001+ employees

Other Solutions Considered

“I'm not sure what solution was used previously before Splunk Enterprise Platform; when I joined this organization, they already had Splunk Enterprise Platform in place..”

Devon Jones

Splunk Engineer

[Read full review](#) 

“Before choosing Splunk Enterprise Platform, I did not evaluate other options; Splunk Enterprise Platform was already selected as a vendor before I started my job..”

Logan Denney

Cyber Security Analyst at a government with 5,001-10,000 employees

[Read full review](#) 

“I know we evaluated options before choosing Splunk Enterprise Platform, but it has been several years ago and I was not involved in that process, so I do not know what the other options were..”

Verified user

Application Server Administrator at a healthcare company with 10,001+ employees

[Read full review](#) 

“Before choosing Splunk Enterprise Platform, I did not evaluate other options because I heard that Splunk Enterprise Platform is the best option and I believe this recommendation from my friends..”

Verified user

[Read full review](#) 

Splunk product manager at a tech vendor with 10,001+ employees

“In my current environment, there was not any solution specifically to do exactly what Splunk is used for now. However, in previous environments that I have worked in, ArcSight had been replaced with Splunk.

“One of the platforms that was evaluated in those environments was Elastic..”

Verified user

[Read full review](#) 

Splunk Engineer at a consultancy with 11-50 employees

“We have typically used tools such as Grafana for metrics, AWS CloudTrail, and AWS CloudWatch logs for viewing logs, but now we have everything centralized in Splunk Enterprise Platform..”

Will Searle

[Read full review](#) 

Director, Consultant

ROI

Real user quotes about their ROI:

“I can't share any exact figures regarding return on investment, but we've had Splunk Enterprise Platform for 15 years, so I would say they're happy with their ROI..”

Verified user

[Read full review](#) 

Information Security Officer at a real estate/law firm with 5,001-10,000 employees

“I cannot speak to that as it is not my daily responsibility, so I am not up to date with those current metrics. I cannot speak to whether I have seen a return on investment..”

Brandon Clark

[Read full review](#) 

Splunk architect at a consultancy with 10,001+ employees

“I have seen a return on investment with Splunk Enterprise Platform as it has saved us time, since I don't have to go and fetch logs from specific tools, as they all come in through Splunk Enterprise Platform..”

Verified user

[Read full review](#) 

Splunk engineer at a outsourcing company with 501-1,000 employees

“I would say we probably do benefit from having Splunk Enterprise Platform because we use it every day and they have expanded our use of it and they have even decided to migrate it into the cloud versus trying to use other open platform systems. We continue to use it, which would tell me that it has been beneficial..”

Justim C

[Read full review](#) 

Network Engineering Operations Manager at a comms service provider with 10,001+ employees

“Because Splunk Enterprise Platform is such a solid product, we only have two admins. One of them is a Linux administrator, which manages the back end, and then there is me, which is the Splunk admin, which is responsible for searches, dashboards, and setting up alerts. We have been able to keep a small team of only two people and have complete oversight over our network and all of our devices..”

Carlos Ciscoor

[Read full review](#) 

IT systems engineer at a outsourcing company with 5,001-10,000 employees

“Without knowing the actual cost, I can say with a very high level of confidence that Splunk Enterprise Platform has provided tremendous value. There are fewer employees needed to perform security assessments, track security events, and manage those types of events. That alone should have been a cost-saving feature, which should have more than returned the value of the initial investment..”

DevonJones

Splunk Engineer

[Read full review](#) 

Use Case

“Splunk Enterprise Platform is primarily used for SOAR in my daily work to ensure everything is making its way there and everything is making its way out.

I verify and track that everything is working smoothly with Splunk Enterprise Platform through alerting..”

Verified user

software engineer at a government with 51-200 employees

[Read full review](#) 

“I am an admin for Splunk Enterprise Platform, so I mostly help other teams use it and enable it. I enable other teams to use dashboards or onboarding different apps and such.

“More recently, we had an onboarding or ingestion of some extra data and as a POC for the HashiCorp app. It was a little challenging because we had to work around some of the different file types and they wanted them coming from specific locations to specific servers. That was a fun thing to do..”

Verified user

IT Monitoring Analyst at a insurance company with 5,001-10,000 employees

[Read full review](#) 

“My main use case for Splunk Enterprise Platform is logging and alerting.

A specific example of how I use Splunk Enterprise Platform for logging and alerting is monitoring server resource utilization as well as uptime and whether servers are offline.

When a server goes offline or resource utilization spikes, an alert is generated and sent via text message to me so that I can respond quickly..”

Kyle Jarius

Cloud Engineer at a construction company with 1,001-5,000 employees

[Read full review](#) 

“The main use case for Splunk Enterprise Platform is collecting logs from across the enterprise and ingesting them so that we can use them to easily search and also for alerting if there are problems with all the different applications and pieces of software that we have installed here.

A simple example of how I use Splunk Enterprise Platform for alerting or searching is if we have a Linux server that is running out of memory. We have the Linux logs in Splunk and then we have an alert set up that if the memory gets below a certain threshold, then it creates a ticket for our team to address it. If the memory gets so low that it is a critical issue, then we get paged that it is an urgent issue we need to take care of..”

Verified user

Application Server Administrator at a healthcare company with 10,001+ employees

[Read full review](#) 

“My main use case for Splunk Enterprise Platform is gaining insights, visibility, and maintenance for on-premise infrastructure.

“For insights, visibility, or maintenance, we have a Splunk forwarder on all of our Windows servers, desktop endpoints, Linux servers, and we collect Cisco switch IOS data. For our CCRI, we are required to collect logs from all those devices. Thanks to Splunk Enterprise Platform and SPL, I was able to write queries that would prove that all of our devices were online, checking in, and reporting. I was also able to show us what is actively online at any given time..”

Carlos Ciscoor

[Read full review](#) 

IT systems engineer at a outsourcing company with 5,001-10,000 employees

I use Splunk Enterprise Platform for log aggregation, data validation, sifting through network connections, building out dashboards, using the dashboards and putting them in Excel to then present to executive people who may not understand the granular details of network connectivity or log ingestion.

In one example, I was investigating some traffic where we were getting hit on one of our servers and we were trying to see where it was coming from and if our managed rule set was working properly as we configured it. Navigating to Splunk Enterprise Platform, I was able to query for all the traffic coming from the nefarious IPs and also grab the locations of where they were going, where they were coming from, and if they were blocked or not. From that, I exported that data into an Excel sheet and used that to build bar charts or pie charts to present to executive leadership on what was going on.

“I think it is a great additive to being in the cloud. As I mentioned, we are an AWS shop. Having Splunk Enterprise Platform has made our lives easier because outside of being engineers, we are all still the analysts as well. We still do all of the investigative work and log analysis. Splunk Enterprise Platform makes it very easy for us to parse and grab data that we would need in a given investigation. I am really happy with the product. .”

Verified user

[Read full review](#) 

cloud security engineer at a tech vendor with 11-50 employees

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.

“Licensing is fairly expensive, especially for any of the premium products. If we choose to go that route, such as Enterprise Security, it is definitely very expensive..”

Logan Denney

[Read full review](#) 

Cyber Security Analyst at a government with 5,001-10,000 employees

“I do not have a full experience with the initial setup, but I do know that for pricing and setup cost, we use Splunk partners that we interact with for that..”

Verified user

[Read full review](#) 

Splunk Engineer at a consultancy with 11-50 employees

“My experience with pricing, setup cost, and licensing is great; I just log in. I was given a login and that is how I worked it. I do not think my department dealt with any of that; that is a whole other department within our organization..”

Justim C

[Read full review](#) 

Network Engineering Operations Manager at a comms service provider with 10,001+ employees

“I have very little experience with pricing, setup cost, and licensing. I handle the engineering and administration of it, not the initial cost and licensing, which are managed by a completely different organization..”

DevonJones

[Read full review](#) 

Splunk Engineer

“The specific metrics my organization has tracked to evaluate the success of reducing total cost of ownership with Splunk Enterprise Platform's non-indexing analytics approach mostly show time saved..”

Verified user

[Read full review](#) 

Splunk product manager at a tech vendor with 10,001+ employees

“My experience with pricing, setup effort, and licensing shows that the price is quite high, specifically becoming quite high if I don't process, change, and filter the data fairly heavily, and the setup effort depends on how unusual the environment is in which or for which Splunk Enterprise Platform is used and which data sources are used..”

Verified user

[Read full review](#) 

Milizsoldat at a tech services company with 5,001-10,000 employees

Customer Service and Support

“The customer support has been acceptable; we had an issue that we thought should be easily solvable or something that works out of the box, but it didn't..”

Verified user

Infrastructure Analyst at a energy/utilities company with 501-1,000 employees

[Read full review](#) 

“The customer support for Splunk Enterprise Platform could be better in that the support agents could be more knowledgeable. It takes a lot of communication to get them on board usually with what we are experiencing..”

Verified user

Application Server Administrator at a healthcare company with 10,001+ employees

[Read full review](#) 

“I have interacted with Splunk support and we have weekly or biweekly meetings with them. It has been great to be able to talk through some of the issues that we have, along with getting some links or putting in a support ticket..”

Verified user

IT Monitoring Analyst at a insurance company with 5,001-10,000 employees

[Read full review](#) 

“Customer support for Splunk Enterprise Platform is great. I have bi-weekly phone calls with Splunk and they are always available to answer my questions and provide suggestions and a way forward for any issues that arise during my deployments. I would rate the customer support a ten..”

Brandon Clark

Splunk architect at a consultancy with 10,001+ employees

[Read full review](#) 

“Customer support for Splunk Enterprise Platform is good, but technical support is variable.

“I would rate customer support an eight on a scale of one to ten..”

Verified user

Information Security Officer at a real estate/law firm with 5,001-10,000 employees

[Read full review](#) 

“Customer support is good. I have always worked well with the account team to ensure that anything needing escalation gets addressed. However, in the last couple of years, the support staff do not necessarily understand the problems I report and sometimes simply regard them as bugs. They expect me to provide diagnostics rather than testing them upfront, which is frustrating, but otherwise, support is very good..”

Will Searle

Director, Consultant

[Read full review](#) 

Other Advice

“My advice to others looking into using Splunk Enterprise Platform is to research the product and utilize all the support that Splunk provides. I have rated this review a ten out of ten..”

Justim C

Network Engineering Operations Manager at a comms service provider with 10,001+ employees

[Read full review](#) 

“I would advise others looking into using Splunk Enterprise Platform to carefully evaluate if there is any less expensive option out there at this time that would do enough of what Splunk Enterprise Platform provides, as it is a very expensive product. I would rate my overall experience with Splunk Enterprise Platform an 8..”

Verified user

Application Server Administrator at a healthcare company with 10,001+ employees

[Read full review](#) 

“I would say look into how you would use Splunk Enterprise Platform and maybe compare other options as well. Also, I have always had a really good experience with Splunk and onboarding has been pretty easy, as well as it being super scalable, allowing you to have great observability. It is really good at self-regulating. Any issues or errors, for example a slowed queue or suddenly ingesting a lot of data, it is really good at regulating itself. I think that is great. I would rate this product a 9 out of 10..”

Verified user

IT Monitoring Analyst at a insurance company with 5,001-10,000 employees

[Read full review](#) 

I think there are always challenges to some things that you learn to build out. It was not anything technical, it was just learning how to manipulate the dashboards and manipulate the data to perform or show how you wanted it to show. Once you figure that out, you can make it as expansive as you would want to.

I would say around AI, everyone needs to improve their governance and security. As great as AI is, it is also scary. While I as the engineer do enjoy having an agentic friend helping me out and making things more efficient, guardrails are still needed to be implemented as we move further into this agentic space.

“I think they are pretty accurate. I have not had any issues at this point, but as we go and continue to do our research and due diligence, I am sure things will get better.

“Continue doing the homework, continue researching, continue using the tool to the best of its capabilities, and building out your data sets as you see fit. I would rate this product a nine out of ten. .”

Verified user

cloud security engineer at a tech vendor with 11-50 employees

[Read full review](#) 

“Regarding Splunk Enterprise Platform's AI capabilities, I find its governance and security intriguing; I do not know a great deal about it, but I have been intrigued by what the possibilities could be.

I am very confident in the accuracy and reliability of output from Splunk Enterprise Platform.

We are not really at the petabyte scale for managing data sovereignty with Splunk Enterprise Platform.

Our use of Splunk Enterprise Platform's Federated Search has evolved for querying data in place; we have expanded it for more visibility for more users, not just IT-based users.

We do not use the trusted control plane within Splunk Enterprise Platform for maintaining granular control over data, so I cannot comment on its effectiveness.

Splunk Enterprise Platform's governance and role-based access controls will be a big part of managing access to our operational data as we consider new use cases such as agentic AI.

My advice for others looking into using Splunk Enterprise Platform is to take your time and learn what you are doing..”

Kyle Jarius

Cloud Engineer at a construction company with 1,001-5,000 employees

[Read full review](#) 

“Regarding Splunk Enterprise Platform's AI capabilities, we have not used it because it is on classified systems, which are air-gapped networks.

“I have not used Federated Search.

“In maintaining granular control over data using the Trusted [Control Plane](#) within Splunk Enterprise Platform, we have a few users from cybersecurity who have everything under the Power User role, and then we have admins. That is all.

“Regarding Splunk Enterprise Platform's approach to managing governance within a private network environment, we use mostly business process as opposed to the technology, so we have not explored that yet, and I would be actually interested in learning about it.

“The advice I would give to others looking into using Splunk Enterprise Platform is to understand that it is closer to a marathon than a sprint. If you are new to Splunk Enterprise Platform, it will take a little time to wrap your head around it and understand it. The value is there and your skills will grow over time, and you should contribute time every day or every week to learning and expanding your knowledge in Splunk Enterprise Platform. It is an excellent product.

“The people in the Splunk world have been awesome. The conference is awesome. Splunk Enterprise Platform is awesome, and the value is awesome. I would rate this review a 9..”

Carlos Ciscaoor

IT systems engineer at a outsourcing company with 5,001-10,000 employees

[Read full review](#) 

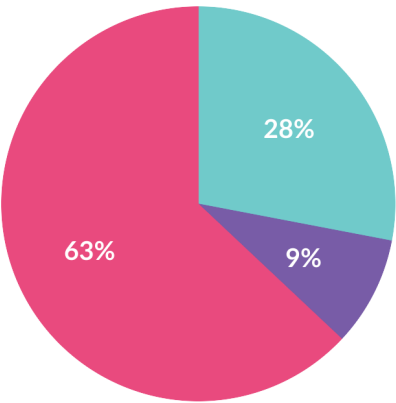
Top Industries

by visitors reading reviews

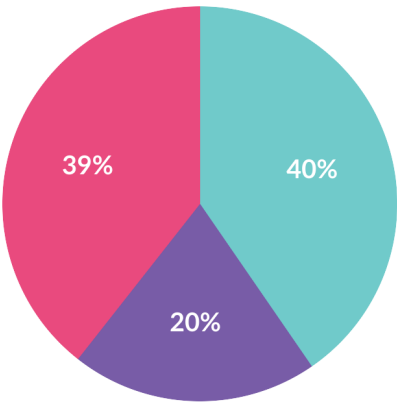


Company Size

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