aws marketplace

Elastic Search

Reviews, tips, and advice from real users






Powered by PeerSpot

Contents

Product Recap

Elastic Search

Elastic Search Recap

Elasticsearch is a prominent open-source search and analytics engine known for its scalability, reliability, and straightforward management. It's a favored choice among enterprises for real-time data search, analysis, and visualization. Open-source Elasticsearch is free, offering a comprehensive feature set and scalability. It allows full control over deployments but requires managing and maintaining the infrastructure. On the other hand, Elastic Cloud provides a managed service with features like automated provisioning, high availability, security, and global reach.

Elasticsearch excels in handling time-sensitive data and complex search requirements across large datasets. Its scalability allows it to handle growing data volumes efficiently, maintaining high performance and fast response times. Integrated with Kibana, Elasticsearch enables powerful data visualization, providing real-time insights crucial for data-driven decision-making.

Elastic Cloud reduces operational overhead and improves scalability and performance, though it comes with associated costs. It is available on your preferred cloud provider — AWS, Azure, or Google Cloud. Customers who want to manage the software themselves, whether on public, private, or hybrid cloud, can download the Elastic Stack.

At its core, Elasticsearch is renowned for its full-text search capabilities, capable of performing complex queries and supporting features like fuzzy matching and auto-complete.

Peer reviews from various professionals highlight its strengths and weaknesses. Pros include its detection and correlation features, flexibility, cloud-readiness, extensibility, and efficient search capabilities. However, users have noted challenges like steep learning curves, data analysis limitations, and integration complexities. The platform is generally viewed as stable and scalable, with varying degrees of satisfaction regarding its usability and feature set.

In summary, Elasticsearch stands out for its high-speed search, scalability, and versatile analytics, making it a go-to solution for organizations managing large datasets. Its adaptability to different enterprise needs, robust community support, and continuous development keep it at the forefront of enterprise search and analytics solutions. However, potential users should be aware of its learning curve and the need for skilled personnel for optimization.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

"Even compared to Splunk, Elastic Search has a good easy-to-use user interface, as even non-technical people can easily search and easily observe the logs and easily track the applications."

Verified user

Senior Software Engineer at a consultancy with 11-50 employees

"My favorite feature is always aggregations and aggregators; you do not have to do multiple queries and it is always optimized for me, and I always got the perfect results because I am using full text search with aliases and keyword search, everything I am performing it, and it always performs out of the box."

Anurag Pal

Technical Lead at YatriPay Limited

"On the subject of pricing, Elastic Search is very cost-efficient, as you can host it on-premises, which would incur zero cost, or take it as a SaaS-based service, where the expenses remain minimal."

Vaibhav Shukla

Staff Software Engineer at Agoda

"Elastic Search is very user-friendly, and we can easily integrate it with third-party models and other AWS S3 buckets."

G Naveen Kumar

Elastic Engineer at The Unique Identification Authority of India (UIDAI)

"What I appreciate about Elastic Search is that the best features include the ability to search through very big documents and index and search through them really fast."

Tom Everson

Product Engineer at A3L

"The best feature of Elastic Search is it does exactly what it says."

MichaelSmith9

CTO at a tech services company with 1-10 employees

"Big businesses cannot survive without Elastic Search because it gives us very good visibility and handles our use cases very well."

Muhammad Mustafa Amin Shah

Lead Engineer at Spidersilk

What users had to say about valuable features:

“Elastic Search is much better, and Kibana is also invaluable. It is scalable, and from my usage, we had many cases where we had to scale it according to the client requirements or the project requirements, and that was very easy because they provide a feature of increasing our usage or the configurations very easily.

“During the first year or year and a half that I was working, it required maintenance. However, with the upcoming migrations and Elastic Search version upgrades, we started automating the alerts and the auto-migrations. The auto-scalability feature of Elastic Search is quite good as well..”

AkashKumar3
Engineer at a outsourcing company with 5,001-10,000 employees

Read full review

“Elastic Search, being a vector database, quickly indexes data, allowing for searches based on text and data directly, which I found fascinating. My dev lead mentioned that it uses C++ to pick up these indexes and pulls up records incredibly fast, in nanoseconds, keeping me interested in how things are becoming faster over time and diversifying away from traditional relational database systems.

Regarding scalability, I consider both vertical and horizontal scalability in theory. I have not experienced sharding but find it interesting as a use case with Elastic Search. I see significant potential for vertical scalability, which can accommodate more data and offer substantial improvement..”

Neel Choudhury
Software Engineer at a tech vendor with 1,001-5,000 employees

Read full review

“What I like the most about Elastic Search is that I can store my data and search throughout my document. It is not like I am doing a search on a particular field only. For example, in comparison with other databases like SQL or NoSQL, you can implement search, but you need to be restricted to a particular field. In Elastic Search, there is an opportunity to search the entire document, and if there are any matches, it gives a score based on which I can decide how much data I need to show.

For example, if I am searching a person's name, there is a chance that the person's name I will be looking for may have some partial match. If I search for Amit, there can be multiple spellings for the same thing. It works on a kind of phonics system, which is a major requirement for me because when people type, they usually make spelling mistakes..”

Shubham Yash Tomar
Principal Engineer at a consultancy with 10,001+ employees

Read full review

“One of Elastic Search's best features is its search capability due to the index-based data management and lifecycle of unstructured data, primarily in the form of JSON, allowing for historical data storage and multiple indexes.

When using traditional keyword and full-text search capabilities, my experience with Elastic Search's performance indicates that the results are obtained much quicker compared to traditional SQL queries, demonstrating superior efficiency.

Elastic Search fulfills my use case requirements effectively, both for my current and previous needs, which is why I rely on it.

Elastic Search positively impacts my company with many benefits across multiple use cases; for example, it enables quick dashboard setups for client reviews and presents data efficiently, ensuring good user experience..”

Manoj Kumar
Solutions Architect at Xebia

Read full review

"For us, what I can notice is the ability of adding weights to each field of the data, which is very useful because sometimes the user searches the data not just by the title, but by specific keywords, and being able to add weight to the fields in order to show that information to the final user is very useful. Also, the panel for showing graphs about the data and how the users are interacting with it is pretty useful.

"The difference in performance of Elastic Search is outstanding; if we compare a traditional database or service for search and index products or, in this case, papers, the difference is outstanding. That is the case when you want to filter the data; the primary advantage will be performance for sure.

"Again, the primary improvement will be performance, and the interactivity we can have with the data is very flexible; it adapts to the needs of the user very easily.

"I cannot see any issues at this point; the panel is great. The way to customize and configure the panel and the search is great; it is really visual. Documentation is great as well.."

Anderson Gil
Software Engineer at Contractor

Read full review

"I chose Elastic Search because it has high search capabilities and setting up the cluster and maintaining it is very easy. Due to this, I found it very user-friendly. High availability and shards allocation are significant advantages that led us to shift to Elastic Search.

"I particularly appreciate the sharding concepts because data has high availability. The semantic search feature and the new logsDB feature are valuable additions. These are things I appreciate most about the platform.

"Semantic search is a very advanced feature that has proven useful for our data in current systems. I am working with Aadhaar, which is a Unique Identification Authentication firm. When we search for name-related terms, the semantic search provides relevant results. I have also implemented semantic features with hospital data, and it has been very useful for multiple cases.

"Elastic Search Hybrid Search is an advanced feature that functions as a future vector database. Vectors are the main component of the database. In current systems, it shows only similar data, but with a vector database, we can store all types of data using vectors. Everything in the future will revolve around vectors. All systems are moving from CPUs to GPUs. This is very useful because comparing vector databases will be a more efficient way to store and retrieve data compared to traditional methods.

"Pricing is very high compared to other solutions, but given the features they provide, the pricing is acceptable. The licensing part is also decent compared to other features. I have no issues with this because the features they provide are excellent and position us for next-level future capabilities.

"Many banks are moving to Elastic Search, and many identification systems are adopting it because the search capability is significantly higher compared to other solutions, and data retrieval is also very efficient. Many industries are transitioning from old solutions like Splunk to Elastic Search. Banking sectors and healthcare sectors are leading this adoption. Many applications use Elastic Search as their backend, such as Zama. Industries are thinking about and adopting Elastic Search technology because of the features it provides.."

G Naveen Kumar

Elastic Engineer at The Unique Identification Authority of India (UIDAI)

Read full review

Other Solutions Considered

"Before choosing Elastic Search, I evaluated other products like Space Cloud and three to four different banking applications, ultimately finding Elastic Search to be the most capable option.."

Manoj Kumar
Solutions Architect at Xebia

Read full review

"Cassandra was one we were evaluating, but we preferred Elastic Search because the documentation was way better and the community was bigger. It is easier to find answers when we face a problem, and that is why we chose Elastic Search.."

Anderson Gil
Software Engineer at Contractor

Read full review

"Before choosing Elastic Search, I evaluated other options. At first, we tried to go with Redis search because we really needed fast retrieval, but Redis search was closed source at that time, so we could not go with Redis search. We had to try Elastic Search and it performed quite surprisingly well.."

Tom Everson
Product Engineer at A3L

Read full review

"I have used other similar solutions to Elastic Search. I think Elastic Search was compared to lexical search or something similar. There is another solution provided by MongoDB which also does similar work; with them, we can restore the JSON format data quickly compared to Elastic Search. MongoDB provides a tool called Compass, and they have Atlas. In Atlas, they are offering a lot of solutions with many features that were missing in Elastic Search. While the searching part in Elastic Search works fine, it lacks a lot of things; for instance, if I need to scale or downgrade my system, the backup restoration works much faster.."

Shubham Yash Tomar
Principal Engineer at a consultancy with 10,001+ employees

Read full review

"Elastic Search is easy to use in Azure cloud. Mostly, my full company uses Azure cloud, so it is easy to use. Cost-wise, my company found Elastic Search is good. Cost matters. Based on cost and use cases, I found Elastic Search is good. Even compared to Splunk, Elastic Search has a good easy-to-use user interface. Even non-technical people can easily search and easily observe the logs and easily track the applications. With Splunk, I found I have to be a little more technical in that area. There are key-based searches and some criteria that I have to remember. I found that difference between Splunk and Elastic Search.."

Verified user

Senior Software Engineer at a consultancy with 11-50 employees

Read full review

"Regarding alternatives, I have worked with various database products, including Azure technologies where I worked with NoSQL storage tables similar to AWS DynamoDB, which are schema-less with varying attributes per record. These use partition key and row key for accessing information, fragmenting what we associate with traditional RDS. Additionally, I worked with Axelor CRM from a French company, alongside MySQL and Oracle. My first company used MS SQL, and I have discussed my use case involving AWS Neptune graph database and Elastic Search, which encompasses all I have worked with so far.."

Neel Choudhury

Software Engineer at a tech vendor with 1,001-5,000 employees

Read full review

ROI

Real user quotes about their ROI:

For time-saving, Elasticsearch is a good software. It is stable, and we do not encounter critical issues like server downtime, which could result in data loss. There are minor misconfigurations regarding data transfer rates that I have noticed sometimes.

FaisalKhan5
SOC A2 at Innodata-ISOGEN

Read full review

"With respect to performance, we have seen a return on investment from Elastic Search. For example, the API response time has improved significantly, cutting the time down from about one or two minutes to around 50% faster, benefiting our downstream applications.."

Bhaskar Kanchi
Consultant at a tech vendor with 10,001+ employees

Read full review

"Estimating the return on investment from Elastic Search is nuanced; however, I can share that initially, search times from traditional RDBMS were around two to three seconds, and with Elastic Search, we reduced that to 50 milliseconds, indicating a significant improvement.."

Vaibhav Shukla
Staff Software Engineer at Agoda

Read full review

"We have not calculated the ROI for Elastic Search, but we are a consumer platform where numerous searches are happening, and we are getting very good results from the current infrastructure of Elastic Search. Though the exact numbers or ROI were never calculated, the performance has been beneficial.."

Chandrakant Bharadwaj
Head of Data Management at Zeno Health

Read full review

"I do not have any specific numbers on a return on investment, but I do have a general sense of the overall improvement of efficiency of the platform as we moved from on-prem hosted to Elastic Cloud on Kubernetes, where the time saved from maintaining the platform itself was significant.."

Louis McCoy
Director, Software Engineering at a tech vendor with 10,001+ employees

Read full review

"I cannot say much about the return on investment part because we normally work on a use case basis. If we find some kind of issue in our database which is currently taking time, then we need to shift to Elastic Search, and it will start giving us very good results. On the cost-saving side, rather than increasing our RDS from a less cluster to a big cluster, we can create a specific separate Elastic Search cluster, and it saves our money on our basic structure while giving us much more performance. I cannot tell you the exact part on how much was saved with the calculation, and I cannot provide the numbers, but it saves our time on the debugging side. Using it on the logs and creating visualization is very convenient for us to search the log and identify the issue as soon as possible. This saves our time, saves the customer's time, and decreases the time to respond and resolve.."

Muhammad Mustafa Amin Shah
Lead Engineer at Spidersilk

Read full review

Use Case

"The major purpose was to solve the search part. We have data in multiple languages, majorly in Indian languages such as English, Hindi, Punjabi, and some Marathi and Bengali. There is a requirement where we need to support a kind of listing, and I can say there is a list of people or users to whom I want to search.."

Shubham Yash Tomar
Principal Engineer at a consultancy with 10,001+ employees

Read full review

"We use Elastic Search for a research application based on paper study, and the primary usage is for indexing the data and then functioning in a similar way to an e-commerce search bar.."

Anderson Gil
Software Engineer at Contractor

Read full review

"My main use cases for Elastic Search involve search capability. For instance, I built a banking product application, the PFM personal information system, requiring search capability and fuzzy search using Elastic Search. Additionally, I use third-party API data to build a super app in the insurance domain, where I collect requests and responses from APIs and store the logs in Elastic Search for debugging purposes, analyzing the data using the Kibana dashboard.

I previously used Space Cloud to build similar functionality; however, it does not support fuzzy search, which is why I switched to Elastic Search for those requirements.."

Manoj Kumar
Solutions Architect at Xebia

Read full review

"I am the Elastic Search admin for my organization, and we are using Elastic Search to handle the traffic to GCP. The monitoring of all the clusters and all the deployments are quite good, and compared to other services such as OpenSearch that we used previously, Elastic Search is much better, and Kibana is also invaluable.

"When we get the logs, it is mostly about how we edit the configurations and how we make changes according to the requirements of our organization. In these cases, the logs sometimes can be a bit inaccurate. We are a customer, and we use Elastic Search integrated into our organization's usage.."

AkashKumar3
Engineer at a outsourcing company with 5,001-10,000 employees

Read full review

"The main use cases are for logging, centralized logging system, and security purposes. We also use it for application monitoring and APM to monitor all the applications that run in our environment.

"Applications developed by some of our users are monitored using APM, which is one of our primary implementations. For security purposes, we centralize logging for all 6,000 servers using Elastic Search. With more than 12,000 servers in our infrastructure, we need to track which server requires attention and receive alerts. For example, if we need to update all servers, some may be missed, but the system will trigger an alert to notify us. Monitoring and logging are the main functions we use in our current systems.

"We are using Elastic Search for log ingestion only.."

G Naveen Kumar
Elastic Engineer at The Unique Identification Authority of India (UIDAI)

Read full review

“I am familiar with Elastic Search to a certain extent as I have used it in my development life. I thought someone wanted feedback about it, specifically how I have used it in my career, so I agreed to share that information.

I started using Elastic Search after becoming acquainted with it when I accessed the AWS environment for the first time during the COVID period. We tried to establish a vertex and edge graph database schema, and I was hired to get that schema up and running while dealing with millions of records related to car spare parts. Due to a signed clause, I cannot go into too much detail. The challenge was with the indexes slowing down, which prompted a move to GraphDB because it provides faster access time. I had to deal with a lot of data cleansing and created many pipelines, first pushing records into Elastic Search through a bulk insert. I also looked up data using Kibana as the front end to leverage queries for pulling up that data.

Once GraphDB was in place, I was required to develop a service for asynchronous processing and order confirmation, where one copy would be stored in a database and the other would be pushed into Elastic Search for further lookup, eliminating the need for direct queries to the RDS

I have never reached out to Elastic Search's technical support team..”

Neel Choudhury
Software Engineer at a tech vendor with 1,001-5,000 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.

"The initial setup process of Elastic Search is straightforward, with comprehensive documentation available for installation guidelines that make it easy for beginners.."

Manoj Kumar

Solutions Architect at Xebia

Read full review

"The initial deployment was something I was not part of for Elastic Search, and even for Mongo not much. However, I have some idea about it; you can create multiple shards and similar configurations. It is easy in both cases.."

Shubham Yash Tomar

Principal Engineer at a consultancy with 10,001+ employees

Read full review

"The initial deployment was fine because the organization already had Elastic Search, and I was not the one who implemented it. I found it easy to get used to the whole usage, so it was fine for me. To fully understand the whole knowledge of all the deployments, it took me about six months, which was a fine timeline according to the requirements of my employer.."

AkashKumar3

Read full review

Engineer at a outsourcing company with 5,001-10,000 employees

"I believe the initial setup for this solution is complex for new members. However, if you are technically strong and understand how Elastic Search systems work, it is very easy. With five years of experience, I have set up many clusters for banking sectors and healthcare sectors. I have built fourteen clusters in production environments with large-scale systems exceeding five terabytes. This will be typical for those who have technical knowledge and can build easily. Those starting without experience can use Elastic Cloud, which offers very easy one-click deployment. They can deploy an Elastic Search cluster with single clicks. Those with technical knowledge can build the cluster themselves, but those without experience can use Elastic Cloud. This is not an issue.."

G Naveen Kumar

Read full review

Elastic Engineer at The Unique Identification Authority of India (UIDAI)

"At first, we faced several issues related to some versioning and allowing indexing the database because part of our information is in a traditional SQL database, and we were using the IDs from the index for the records in Elastic Search. We created a little ETL for that, and handling that process was tricky and harder at first. That was the biggest challenge we faced when starting to set up Elastic Search.

"I would say that first, contact support for the initial setup; I think it will make the process easier. Then start, for example, with how to send and retrieve the data in the documentation; I think that is the best thing they can do.."

Anderson Gil

Software Engineer at Contractor

Read full review

"When discussing initial deployment, the specific attribute of interest is the overall initial installation when starting to roll out the product. The deployment was a struggle as I faced challenges with bash commands and understanding how to run things on my system. Looking up tutorials on YouTube was tricky, and cross-referencing with documentation posed difficulties as some people customize setups to their needs. Setting up MySQL is straightforward, while with Elastic Search, I had to run bash commands for proper service execution. I faced some hurdles getting CRUD queries to work correctly. I resorted to Docker as an alternative, which diverged from standard practices of creating a local database service. An ideal setup would include a setup executable for Windows that would greatly facilitate immediate access and CRUD operation starts.

In my case, the system was already running by the time I started, as the custom DevOps team managed the deployment, and I was only tasked with connecting via Kibana and issuing bulk insert commands.."

Neel Choudhury

Software Engineer at a tech vendor with 1,001-5,000 employees

Read full review

Customer Service and Support

"Technical support for Elastic Search is satisfactory, with quick solutions provided by support teams and active open forums available. I rate customer service and technical support as an eight out of ten.."

Manoj Kumar
Solutions Architect at Xebia

Read full review

"I do not know anything about the tech support because I have not escalated any questions to the technical support or customer service teams. We have not talked to anyone.."

Tom Everson
Product Engineer at A3L

Read full review

"I have contacted technical support or customer support several times, but not me personally; my DevOps team has connected with the technical support several times. They deal with the contact support because they handle all the infrastructure setup and issues related to DevOps.."

Shubham Yash Tomar
Principal Engineer at a consultancy with 10,001+ employees

Read full review

"I have raised ticket sizes with them many times. I feel very supported by their customer service. For P1 tickets, they provide very immediate quick responses and join calls to support and troubleshoot the issue accordingly. They provide solutions very efficiently. Their service is very good.."

G Naveen Kumar
Elastic Engineer at The Unique Identification Authority of India (UIDAI)

Read full review

"We are in constant contact with technical support because we have a large amount of projects in our wing. Mostly, in order to check what the backend situations are, we contact technical support, which is quite easy to reach. Once there is any case that requires a one-on-one interaction, it is easy to contact them and we have a session to resolve the issue. The technical support is great.."

AkashKumar3
Engineer at a outsourcing company with 5,001-10,000 employees

Read full review

"Support-wise, it is good because I did not get much support work. Mostly my DevOps team handles it, but one or two times I did get support. There is a ticket creation option. Within the available time zone, somebody will be there to support me. Within two to three hours, somebody can help and try to resolve the issue.

"Sometimes, engineers take time to assign when I create a ticket.."

Verified user

Senior Software Engineer at a consultancy with 11-50 employees

Read full review

Other Advice

"For implementing Elastic Search, I would say good documentation, and it is really easy to use. We have an example of almost every functionality that is inside of Elastic Search framework, so that is helpful. I would provide a rating of ten for this product, and I say a ten; it is really good.."

Anderson Gil
Software Engineer at Contractor

Read full review

"Elastic Search overall is good. Regarding relevancy and searching, the searching is fine because in my use case, we only use it to retrieve the data, and the text search is quite good. We do not find any issue with that. In Elastic Cloud, which comes with the premium enterprise version of Elastic Search, we just got that this year. We received it in January, and they have inbuilt tools for GenAI. They also have a RAG feature where we can get LLMs to find answers or generate data, and that was quite good. I would give Elastic Search a rating of seven overall.."

AkashKumar3
Engineer at a outsourcing company with 5,001-10,000 employees

Read full review

"For an overall rating of Elastic Search, I would score it at a solid 8 out of 10.

Its speed has facilitated my understanding of logical operators and streamlined query issuance. I would love to grasp the inner workings of sharding with distributed schema implications. Based on what I have experienced thus far, I find

it a significant improvement, but once I better understand sharding and its performance effects, I would likely adjust my score.

My experience with the relevancy of search results using Elastic Search indicates that issuing a full query yields a finite number of results, while partial text searches can return irrelevant information. Mastering query issuance with Elastic Search is a valuable skill that develops over time. I prefer a structured JSON approach, utilizing properly sequenced clauses, which allow drilling down to a limited set of records that directly relate to the search context.

On hybrid search effectiveness, I think that AI is progressively offering more concise information. Providing more relevant keywords allows Elastic Search to generate results faster than other databases, such as RDS. The ability to engage with text directly simplifies understanding records and has a significant impact on AI functionality in rendering accurate results based on user needs..”

Neel Choudhury
Software Engineer at a tech vendor with 1,001-5,000 employees

Read full review

"Correlation alerts is a feature I did not get the opportunity to work on. I have only theoretical knowledge but not practical knowledge.

"We can use agentless approaches with a script in addition to agent-based approaches. We are building both agentless and agent-based solutions. Both are good. Agent-based approaches for fetching data work well. Both are functioning well.

"Discovery is a feature we are using, and it works well. Attack is a feature I did not get the opportunity to try.

"Elastic Search is very user-friendly, and we can easily integrate it with third-party models and other AWS S3 buckets. It is very user-friendly for integrating with other third-party tools.

"My overall review rating for this solution is ten out of ten.."

G Naveen Kumar
Elastic Engineer at The Unique Identification Authority of India (UIDAI)

Read full review

"A lot of maintenance is required on my end. A lot of data needs to be synced because we were using CDC, so a lot of data is transmitted from my primary database to this secondary database for searching purposes. That requires a lot of effort. However, using the cloud solution, I think it can be set up; but again, it costs me a lot.

My experience with the relevancy of the search results when using traditional keyword and full-text search capabilities shows that as we are moving towards AI, you can keep all your data and break it into an AI format. Whatever I want to search, it will give me a result. I think moving forward, plain text search will not be a long-term solution because as people are moving towards AI, they want machines to understand better what they are trying to search. For example, I may

want to search for a person based on department and years of experience, and for that, I think Elastic Search will suffice. However, breaking data into tokens and embedding it for querying will be a better solution moving forward. Elastic Search is also providing some sort of AI solution, but I have not had much time to explore that yet.

I believe the effectiveness of hybrid search, which combines vector and text searches, is great because vector search deducts information from the text provided to a machine and effectively gives the related data. If I use vector search with plain text in a hybrid search, it will be a better solution moving forward. This is because people do not want to search for something such as Atul Kumar; they want to search for Atul Kumar from a specific department or company, region, or city. My overall rating for this product is eight point five out of ten.."

Shubham Yash Tomar
Principal Engineer at a consultancy with 10,001+ employees

Read full review

"I am currently using Elastic Cloud Serverless.

My application is hosted on AWS cloud, utilizing managed services including the open search, which is a component of Elastic Search.

I use the ELK stack for log ingestion and visualization of application logs via Kibana.

I find that the ability to parse and structure raw logs without agents requires different approaches for each use case.

I am using the Attack Discovery feature.

The discovery feature helps me correlate alerts by writing custom queries to

retrieve logs based on specific criteria.

I utilize generative AI models like Claude AI and Anthropic within the discovery context for better log analysis.

From a technical point of view, integrating AI capabilities within Elastic Search enhances its value, showcasing the potential for using models and RAG in my systems.

I recommend Elastic Search for companies with substantial data needs or searching requirements, considering it the best search engine. I have provided an overall review rating of nine out of ten.."

Manoj Kumar
Solutions Architect at Xebia

Read full review

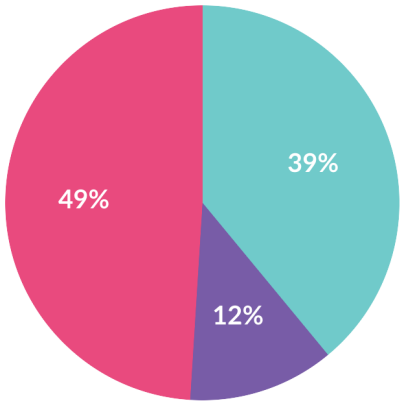
Top Industries

by visitors reading reviews

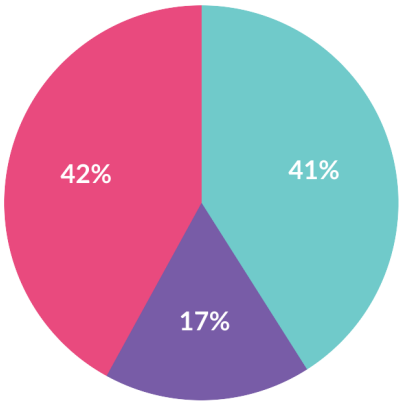
Financial Services Firm	11%
Outsourcing Company	9%
Manufacturing Company	9%
Comms Service Provider	7%

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 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