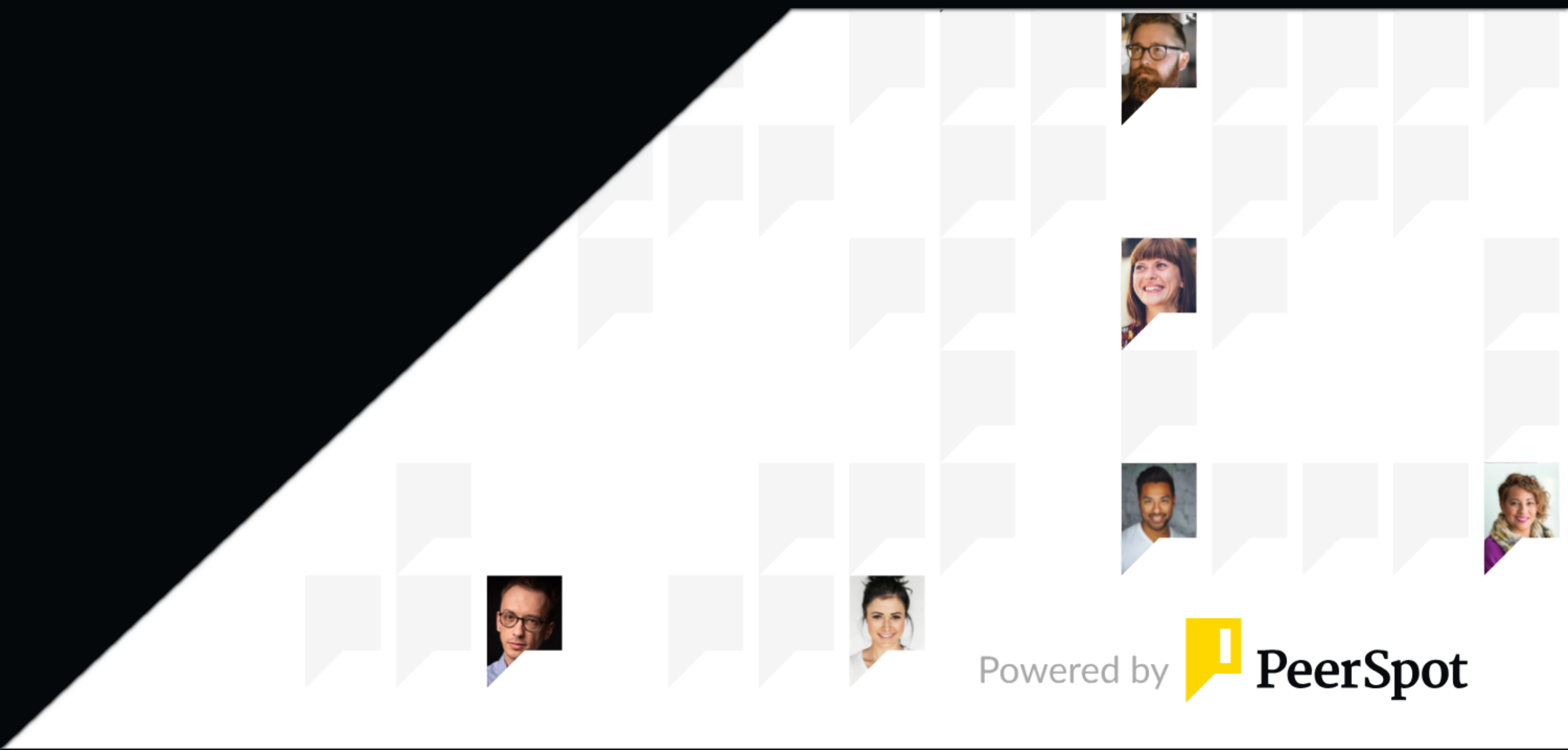
aws marketplace

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:

✓ “Elastic Search is very quick when handling a large volume of data.”

Naresh Modhwadia

Software Engineer at Government of India

✓ “Overall, considering key aspects like cost, learning curve, and data indexing architecture, Elasticsearch is a very good tool.”

FaisalKhan2

SOC Analyst at Silverse

✓ “I find the solution to be fast.”

Abdul Rahaman Abdul Rahim Lee

BI and Analytics Engineer at Sandvine Inc

✓ “The stability of Elasticsearch was very high, and I would rate it a ten.”

Verified user

Backend Developer

✓ “The full text search capabilities in Elastic Search have proven to be extremely valuable for our operations.”

Himanshu Bhati

Senior Devops Engineer at Ubique Digital LTD

✓ “All the quality features are there. There are about 60 to 70 reports available.”

Anand_Kumar

Enterprise Architect at DXC Technology

✓ “Logsign provides us with the capability to execute multiple queries according to our requirements. The indexing is very high, making it effective for storing and retrieving logs. The real-time analytics with Elastic benefits us due to the huge traffic volume in our organization, which reaches up to 60,000 requests per second. With logs of approximately 25 GB per day, manually analyzing traffic behavior, payloads, headers, user agents, and other details is impractical.”

Saurav Kumar

Senior security architecture at National Payment Corporation Of India

What users had to say about valuable features:

“I appreciate the indexing capabilities and the speed of indexing in their product, which demonstrates how quickly logs are collected and stored. The search capabilities are also valuable..”

PH Chiu
Consultant at a tech services company with 51-200 employees

Read full review

The most valuable feature of Elasticsearch was the quick search capability, allowing us to search by any criteria needed. The searches were executed very quickly, which made the process reliable. Additionally, full-text queries were integral to our usage. Our productivity was consistently maintained with this database. Its consistent performance allowed us to maintain steady productivity levels.

Verified user
Backend Developer

Read full review

Configuring Elasticsearch is much easier compared to comprehending other SIEM tools like Splunk. It has a full command-based access that allows you to configure how much data you want to store and set up retention policies. I can easily change the bandwidth for the network to send log data. Elasticsearch is quite user-friendly and offers a hands-on experience for configuring databases.

FaisalKhan2
SOC Analyst at Silverse

Read full review

"I find the solution to be fast. Aggregation is faster than querying directly from a database, like Postgres or Vertica. It's much faster if I want to do aggregation. These features allow me to store logs and find anomalies effectively.."

Abdul Rahaman Abdul Rahim Lee
BI and Analytics Engineer at Sandvine Inc

Read full review

"Elastic Search provides features such as stemming and range-based queries to search log files efficiently. It allows filtering data easily by searching for specific words based on created indexes. This made searches very efficient, and it also allows for log collection through Kafka and helps with managing logs and customizing searches according to needs, such as grouping by dates or user IDs.."

Verified user
Sr. Consultant at a computer software company with 51-200 employees

Read full review

When discussing the features of Elastic Search, the full text search capabilities are particularly beneficial for handling large volumes of data.

The full text search capabilities in Elastic Search have proven to be extremely valuable for our operations.

“Regarding AI integration, we have not yet implemented any AI-driven projects or initiatives using Elastic Search..”

Himanshu Bhati
Senior Devops Engineer at Ubique Digital LTD

Read full review

Other Solutions Considered

“I used a different solution before switching to Elastic Search because Elastic Search offered a wider range of features. The other solution focused on monitoring app usage, Elastic Search stood out with its extensive modules, cloud deployment options, and flexible monitoring capabilities. Despite Splunk being a bigger name, I found Elastic Search to be more versatile and enjoyed using it..”

Randy Sanchez
Consultant at High Key Consulting llc

Read full review ↗

“I remember Apache Solr, which is generally used for much larger scale data compared to Elastic Search. Apache Solr is used by most companies, and while Elastic Search is very common, there are technologies similar to Elastic Search, though I'm not familiar with all the names..”

Verified user
Sr. Consultant at a computer software company with 51-200 employees

Read full review ↗

“Our experience has been positive, finding solutions in documentation without needing customer support. We also use supporting technologies like PostgreSQL, Spring Boot, and Subversion for seamless integration. .”

Naresh Modhwadia
Software Engineer at Government of India

Read full review ↗

“We've explored a few alternatives, but I believe Elasticsearch, particularly with Elastic and Elastic Cloud, stands out as the current industry standard. Opting for a widely used platform is advantageous due to the larger community it attracts. A substantial user base means more people to consult, numerous information sources, and a wealth of case studies. While there are smaller, medium, and even large alternatives, having around eighty percent of the community share provides a significant pool of expertise and resources to tap into..”

Dave Ezrakhovich
Site Reliability Engineering at WiseTech Global

Read full review ↗

I have experience with Delinea, ManageEngine, BeyondTrust, IBM and WALLIX. But compared to Elastic, they lack the same level of artificial intelligence capabilities. It's like an all-encompassing package with tons of features. One of those features is the ability to pinpoint the root cause of any problem, whether it's code issues (like it was not written properly), developer errors, or anything else. It goes beyond just surface-level troubleshooting and digs deep to give you the real why. That's what sets it apart from the others. Imagine an application is having some issues. Elastic can tell if it's faulty code, a developer mistake, or anything else. It gives you the true root cause, not just the surface-level symptoms. That's its strength and why it stands out as the industry standard.

PHILIP OLANIYAN
Relationship Manager at Snapnet Ltd

Read full review

"I tried to sell Kibana twice, but in terms of deployment, we've used it in two or three places. However, I don't have hands-on experience with Kibana.

To be very honest, we faced some setbacks with Kibana, particularly with network-level monitoring. This issue occurred a few weeks ago when I tried to sell one of our products. We have used Kibana for APM purposes, as well as the Elasticsearch ELK stack.

From an application perspective, it's one of the tools we use. I can share a lot of insights, but I haven't seen all their reports or dashboards. So, my experience is from a presales perspective rather than a deployment perspective.

If I compare it with other auxiliary tools like Dynatrace, SolarWinds, or Relay, Elasticsearch is very competitive and user-friendly.

One thing about Elasticsearch is the way they sell licenses for their database, which can be a bit hidden. Many people think Elasticsearch is entirely open-source, but there are charges involved. It's an MPP-based NoSQL database with some limitations on certain datasets.."

Anand_Kumar
Enterprise Architect at DXC Technology

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.

FaisalKhan2
SOC Analyst at Silverse

Read full review

"Our organization prioritizes open-source tools. We have not purchased any licensed products, and our use of Elastic Search is purely open-source, contributing positively to our ROI. We adopt open-source tools due to the organization's policy.."

Naresh Modhwadia
Software Engineer at Government of India

Read full review

"Elastic Search has provided a valuable return on investment by enhancing effectiveness and aiding in learning about security features. It has saved me an estimated couple of hundred dollars in both time and money.."

Randy Sanchez
Consultant at High Key Consulting llc

Read full review ↗

"A stack like Elasticsearch that enables heavy lifting of the data effortlessly comes with its intrinsic yet obvious ROI. If one is not able to realise the ROI it means either the data is bad (garbage in, garbage out) or the stack is not implemented properly.."

Kiran BM
Chief Data Scientist at Everlytics Data Science Pte Ltd

Read full review ↗

"It seems good in terms of return on investment. It is a monitoring solution, and it triggers alerts before something happens. For example, it triggers an alert when the space in Windows reaches an 80% limit. I would say it is a good investment. We are able to fix things before they go wrong. If we didn't have Elasticsearch, things would go wrong, and we would be spending more time fixing them later on.."

Ayesha Imtiaz
Senior Analyst at a tech services company with 10,001+ employees

Read full review ↗

Use Case

Our primary use case was primarily for data storage and quick searching. We focused on getting objects from the database and filtering them efficiently. This involved getting and searching through objects.

Verified user
Backend Developer

Read full review

"The primary use case for Elasticsearch is to serve as a non-SQL database platform to replace traditional SQL processes. It is used in situations where unstructured data needs to be studied and searched.."

Yu-Lin Lee
Sr. Threat Researcher at Trend Micro

Read full review

"I am an end user, and we use Elasticsearch for our logs. Specifically, we use it for security logs for our enterprise, including machines, networks, and endpoints, as part of our IT infrastructure.."

Verified user
Information Security Engineer at a financial services firm with 11-50 employees

Read full review

“We are using Elastic Search for free text search. We scan cache files and convert them into OCR. This allows our end users to search for any judgment given in the 1980s or 1990s based on their criteria. .”

Naresh Modhwadia

Software Engineer at Government of India

Read full review

“At Shopee, I worked with numerous database schemas to find out which table columns belonged to which schema. We utilized Elastic Search to manage metadata for millions of tables, allowing us to search efficiently. Besides that, we used Logstash to put all the log files in Elastic Search for easy searchability..”

Verified user

Sr. Consultant at a computer software company with 51-200 employees

Read full review

I have used the Wazuh SIEM tool, an open-source SIEM tool that uses Elasticsearch for indexing. In this SIEM tool, we have a large amount of logs. Data are converted into alerts, then they are stored in our environment for monitoring and security purposes. For storing that data in Wazuh, we use Elasticsearch indexing.

FaisalKhan2

SOC Analyst at Silverse

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 is not complex. The only part that may require specific knowledge is communicating your cloud environment with New Relic and managing the cloud environment configurations.."

Anderson Linares

Solution ingenier at Quipux S.A.S do Brasil

Read full review

"The product's setup is difficult, since you need at least 5 servers in a distributed topology to achieve its full potential: 3 machines for elasticsearch, 1 for logstash and another for kibana."

André Luiz Girol

Engineering Manager at MaisTODOS

Read full review

"

The deployment is easier for experienced but beginners may face difficulties during installation. They could easily outline the recommended steps for deployment.

Saurav Kumar

Senior security architecture at National Payment Corporation Of India

Read full review ↗

The complexity of the initial setup depends on the requirements. In an MSSP scenario, where multiple clients use the same software, there is a need to segregate the data. This can make the setup more complex, especially for a single client where you need to adjust network configurations.

FaisalKhan2

SOC Analyst at Silverse

Read full review ↗

“The initial setup for the SaaS platform is quite easy. We took assistance from an engineer for the onboarding. Thus, it was straightforward for us. However, there could be a better integration with AWS.

I rate the process a seven out of ten..”

Verified user

Solutions Architect at a recruiting/HR firm with 1-10 employees

Read full review

“I would rate my experience with the initial setup a nine out of ten, with ten being easy. It is easy, not that difficult.

It can be deployed both on the cloud and on-premises. I've seen on-premises deployments. This is especially true in other parts of the world where governments don't want to use the private cloud and have their own private cloud. I have mostly worked with on-premises deployments.

The mapping can take three months on average. However, the deployment time depends on the project. If you have a hundred servers, it will take two or three weeks. With three or four thousand servers, it will take longer. It's the same with any tool, like Dynatrace or SolarWinds. We have to map services and events, set thresholds, and configure event triggering and notifications. There's a lot to consider, so it depends on the project scope, the number of servers, the data captured, and whether it's agent or agentless. It's difficult to calculate an average about how many days it will take..”

Anand_Kumar

Enterprise Architect at DXC Technology

Read full review

Customer Service and Support

“I've never heard anything wrong from the delivery side, but it's an international company with a very good product. So, the support system should be good..”

Anand_Kumar
Enterprise Architect at DXC Technology

Read full review ↗

“Till date, we did not have any issues with customer service and support. Like, initially, we had issues in accessing the portal. But that was the only issue, but it was resolved pretty quick..”

Verified user
Founder at a tech services company with 11-50 employees

Read full review ↗

“We subscribed to NGINX for technical support, and they were helpful during the installation phase. There is a lack of community support for GRPC, which needs improvement. .”

Saurav Kumar
Senior security architecture at National Payment Corporation Of India

Read full review ↗

“Their documentation is commendable as it provides a clear understanding of their offerings. Also, the accessibility to their support further enhances user-friendliness, making it a straightforward and user-friendly experience. While it may be slow, their competence in what they do is evident. I would rate it eight out of ten..”

Dave Ezrakhovich
Site Reliability Engineering at WiseTech Global

Read full review ↗

“I would rate technical support from Elastic Search as three out of ten.

“The main issue is a general sum of all factors. Being based in Hong Kong means I can only assess the service in my region and cannot speak for other regions based on my experience..”

PH Chiu
Consultant at a tech services company with 51-200 employees

Read full review ↗

“Most of our deployments are not exposed to the Internet or public networks; they're restricted to closed networks. We don’t frequently upgrade from previous versions unless a specific use case arises.

In such cases, we usually turn to the developer community for support.

Another scenario is when running the application in a careful mode, where the main requirement is to change the image name in the configuration. Then, we check for any changes or incompatibilities with previous versions. Upgrades can sometimes introduce issues if they’re not compatible with existing configuration files, but it's generally not too problematic to handle..”

Atif Tariq
Cloud and Big Data Engineer | Developer at Huawei Cloud Middle East

Read full review

Other Advice

If a feature for renaming indices could be added without affecting the performance of all other features, it would be nice to have. Overall, I rate Elasticsearch a ten out of ten.

Verified user
Backend Developer

Read full review

Overall, considering key aspects like cost, learning curve, and data indexing architecture, Elasticsearch is a very good tool. I would rate it as a nine.

FaisalKhan2
SOC Analyst at Silverse

Read full review

“I have used Elastic Search, but I might not be aware of many internal details; I just used the API to create an index, manage data, and search. It's very useful. On a scale of 1-10, I rate it an eight..”

Verified user
Sr. Consultant at a computer software company with 51-200 employees

Read full review

“For someone wanting to be a security analyst, Elasticsearch is a valuable tool. It helps organizations collect large amounts of logs from various platforms like

Windows, Ubuntu, and Palo Alto Networks.

I'd rate the solution eight out of ten..”

Verified user
Information Security Engineer at a financial services firm with 11-50 employees

Read full review ↗

I previously used Graylog.

I am currently working with Elastic Search as the primary solution.

“My role is Senior DevOps engineer at UVIK Digital.

“On a scale of 1 to 10, with 10 being the highest, I would rate Elastic Search as an 8 overall as a product and solution..”

Himanshu Bhati
Senior Devops Engineer at Ubique Digital LTD

Read full review ↗

“The real-time analytics capabilities depend on whether you use the paid version or open-source version.

“I work with SME users of Elastic Search, though the solution can technically support enterprise customers.

“I have not extensively used AI technology with Elastic Search.

“I can recommend Elastic Search to other users.

“The pricing for Elastic Search rates as four out of ten. Overall, I would rate Elastic Search as seven out of ten..”

PH Chiu
Consultant at a tech services company with 51-200 employees

Read full review

Top Industries

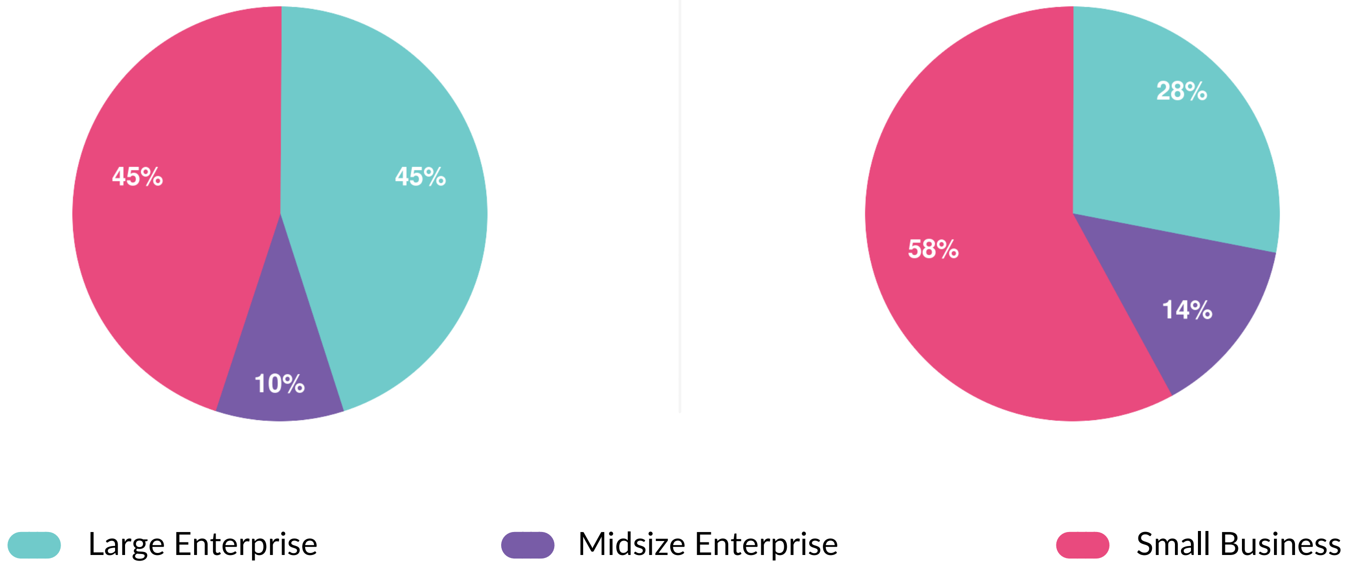
by visitors reading reviews

Computer Software Company	14%
Financial Services Firm	13%
Government	9%
Manufacturing Company	8%

Company Size

by reviewers

by visitors reading reviews



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