

aws marketplace

Cybersixgill

Reviews, tips, and advice from real users



Powered by  PeerSpot

Contents

Product Recap..... 3 - 4

Valuable Features..... 5 - 10

Other Solutions Considered..... 11 - 14

ROI..... 15 - 16

Use Case..... 17 - 18

Setup..... 19 - 21

Customer Service and Support..... 22 - 23

Other Advice..... 24 - 26

Trends..... 27 - 28

About PeerSpot..... 29 - 30

Product Recap



Cybersixgill

Cybersixgill Recap

Cybersixgill empowers organizations with cyber intelligence by monitoring open sources and dark web activities, tracking threat exposure, and assessing risks without on-premises infrastructure.

Cybersixgill enables powerful intelligence gathering by providing access to a comprehensive data lake of deep and dark web activity, identifying trends in malware, and analyzing underground markets. Organizations can monitor illegal activities like credit card sales and conduct searches on hacker forums using its API and Investigative Portal. Automatic translations and alerts enhance threat detection, making it a vital tool for real-time cybersecurity management. Users have expressed a desire for better real-time updates and improved data source coverage along with more user-friendly query specificity and training materials.

What are the key features of Cybersixgill?

- **Investigative Portal:** Empowers teams with contextual, actionable alerts and covert investigation capabilities.
- **Data Lake:** Leverages the largest collection of deep and dark web activity for comprehensive threat analysis.
- **Advanced Search:** Utilizes operators for specific queries and tracking leaked credentials efficiently.
- **Real-time Alerts:** Provides instant notifications customized to organizational needs.
- **Threat Actor Profiling:** Examines profiles, methods, and histories to understand risks comprehensively.

What benefits should users look for in reviews?

- **Time Savings:** Streamlined information gathering reduces the need for multiple analysts.
- **Risk Mitigation:** Identifying threats early lowers potential impacts and enhances security posture.
- **Enhanced Coverage:** Broad access to deep and dark web data enriches intelligence capabilities.
- **Return on Investment:** Effective threat detection and response minimize potential losses.

Cybersixgill's cybersecurity solutions are critical in sectors like finance, healthcare, and retail where sensitive data protection is paramount. Organizations leverage the platform to proactively detect threats and safeguard customer information, significantly reducing the risk of data breaches and fraud while maintaining industry compliance.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- ✓ “The solution’s approach of using limited open source intelligence and focusing, instead, on the Deep Web and Dark Web is what seals the deal. That is why I like them. I have other tools that I can aggregate all the open source intelligence from. I value Cybersixgill because it provides access to things that no one else does.”



Verified user

Lead Cyber Threat-Intelligence Analyst at a educational organization with 10,001+ employees

- ✓ “To be diligent for the customer, we usually go into Cybersixgill Investigative Portal to analyze and search things. The solution tells us the reputation of cyber threat actors. So, if someone has a reputation of one, it is a really bad idea to care about what that person is saying. However, if you find someone with a reputation of nine, then there is a high probability that we need to address the problem. You can get information about these type of actors in Cybersixgill Investigative Portal. They have a huge collection, which is like having the rules/goals of the dark web and deep web without having to go there. Our analysts avoid going dark web because they have Cybersixgill Investigative Portal and can get the news from their browser, searching wherever they want.”



Verified user

Head of Cyber Intelligence at a tech services company with 501-1,000 employees

- ✓ “The advanced analysis has made our security operations more efficient. It has also potentially given us quicker access to data that we might not have otherwise located.”



Verified user

General Manager - Cyber Security at a consultancy with 11-50 employees

- ✓ “They also provide some of the greatest notification capabilities. I put in a customer's company name and domain names, or sometimes I put in their IP addresses as a keyword. Once Sixgill collects information that includes those keywords, they then provide us email notifications. That means we can catch information related to our customers as soon as possible.”



Verified user

Manager of Cyber Intelligence Center at a consultancy with 10,001+ employees

What users had to say about valuable features:

“We can easily conduct searches on leaked credentials. It gives us the ability to look at a timeline and build profiles against companies that we are trying to protect, then track changes to credentials or leaking bucket/cloud services associated with those companies. That is the benefit for us. A lot of it is stuff that we can do manually, but it is more about the time it takes as well as the number of analysts you need to do it compared to getting it provided as a quick service.

It is scalable in that we don't need a dozen people to do the work. With this tool, one person can do it..”

Verified user

[Read full review](#) 

General Manager - Cyber Security at a consultancy with 11-50 employees

“In the search engine, you are able to use operators. These operators allow you to do specific searches or open searches. The main things are:

- If you want to search everything related to a specific malware family but you don't want to have anything related to specific search. So, you can just upload it from the search engine and search for it.
- If you only wanted to know about one specific vulnerability, but you don't care what is in Telegram or GitHub as repositories, then it will only care for these things in the dark web forums. You can narrow your search to that.
- If you want only sites in Spanish, but not in other languages, you can narrow your search to that.

There are a lot of possibilities when using the search engine. It has become really useful for my analysts.

The solution has enabled us to access sources that we have not seen anywhere else, such as Telegram. It also gives us access to the Genesis Marketplace. Otherwise, we would have to pay someone for that. However, with Cybersixgill, we can go to the platform and search for whatever we want. .”

Verified user[Read full review](#) 

Head of Cyber Intelligence at a tech services company with 501-1,000 employees

“One of the most valuable features is the ability to be alerted to any possible imminent attack, or mention of your organization by a possible attacker.

It is also of the highest importance that it runs on a collection of Deep Web, Dark Web, and closed sources. This tool is a must for any organization that has a large footprint. The solution’s approach of using limited open source intelligence and focusing, instead, on the Deep Web and Dark Web is what seals the deal. That is why I like them. I have other tools that I can aggregate all the open source intelligence from. I value Cybersixgill because it provides access to things that no one else does. And the tool is configured to do this in a way that provides advanced analysis. That is one of the main values that it provides. They are not just aggregating open source news and feeds, they're actually gaining access to real intelligence.

The size and scope of the solution's collection are pretty impressive. I am impressed with the ease through which the tool allows you to track threat actors who are likely to target you, on a variety of underground forums which are closed. These are sources that would require a solid effort to infiltrate. The automatic translation of any exchange within the platform makes it the most expedient solution for automated threat intelligence and chatter monitoring.

Cybersixgill has also enabled us to access sources which we have not seen anywhere else. They have access to closed forums that I don't want to mention, but that access is important because it's not available anywhere else..”

Verified user

[Read full review](#) 

Lead Cyber Threat-Intelligence Analyst at a educational organization with 10,001+ employees

“One of their strong points is flexibility. That means that once I log in to the Sixgill portal, I can search anything with a specific enquiry. Sixgill provides dark web information based on the search query. By using a combination of the queries, we can exclude various information. It's a very powerful feature of Sixgill.

Regarding the solution's scope, they already provide many things, and they are gradually extending their coverage. They also cover Twitter, Reddit, and some social media. The only thing they don't cover is security news from open sources.

They also provide some of the greatest notification capabilities. I put in a customer's company name and domain names, or sometimes I put in their IP addresses as a keyword. Once Sixgill collects information that includes those keywords, they then provide us email notifications. That means we can catch information related to our customers as soon as possible. Sometimes threat actors share vulnerable website leaks, and if one contains a client's assets, we can catch it quickly and notify the client.

Sixgill also provides threat actor analysis capabilities. When we catch some information regarding a client, such as when some dark web forum member mentions a client's asset, before we report it to the client we conduct a threat actor analysis. Not all members of dark web forums are serial cyber criminals. There are also some kids. Sixgill's threat actor analysis capability provides us with that threat actor's reputation on the forum and helps us know whether a post is very serious or not. We can understand who the threat actor is and whether he is a serious hacker or not. It's very useful information..”

Verified user[Read full review](#) 

Manager of Cyber Intelligence Center at a consultancy with 10,001+ employees

Other Solutions Considered

“Before Cybersixgill, I would use open source tools and my own access to Dark Web forums. I would use GitHub tools and my own investigation on Dark Web forums, and it would take an enormous amount of time. Once I found this solution, I saw that I can do it all within one platform, easily..”

Verified user

Lead Cyber Threat-Intelligence Analyst at a educational organization with 10,001+ employees

[Read full review](#) 

“Before Cybersixgill Investigative Portal, we were doing it old school.

We were at an RSA conference in San Francisco where we spoke to the Cybersixgill guys. They demonstrated the solution and we liked what we saw..”

Verified user


General Manager - Cyber Security at a consultancy with 11-50 employees

[Read full review](#) 

“We didn't really see any comparable options at the time that we evaluated it. Since then, we have seen a couple of others, but I still think Cybersixgill Investigative Portal is probably the best of the ones that I have seen, more from the user interface than anything and the way it presents the data. Cybersixgill Investigative Portal has a clean user interface that is fairly easy to use. Whilst there are other tools that provide access to similar systems, this solution is more about the ease of use.

We also looked at Farsight..”

Verified user

[Read full review](#) 

General Manager - Cyber Security at a consultancy with 11-50 employees

“I have some prior experience with competitors of Sixgill, such as Recorded Future, IntSights, and FlashPoint. I have also tested some similar solutions.

Compared with other solutions, Sixgill's main strength is flexibility. Other solutions, such as Record Future and FlashPoint, sometimes have difficulty receiving load information. Load information means what is actually posted on a forum. By using Sixgill I can get exact information from posts on underground forums. Some of the other solutions lack information. That is why I use Sixgill, after comparing it with those platforms..”

Verified user

[Read full review](#) 

Manager of Cyber Intelligence Center at a consultancy with 10,001+ employees

“It is very important that the solution runs on a collection of deep web, dark web, and closed sources. I have other platforms for other kinds of stuff. I have Cybersixgill only because of its capacity to have information regarding the deep web and dark web. That is its main feature.

The size and scope of the solution’s collection is amazing. I have tested different solutions and Cybersixgill Investigative Portal is the one that has the most information regarding the deep web and dark web. They have a huge collection.

I have tested out other solutions. When we compare what they can and cannot do, we see how Cybersixgill Investigative Portal is superior in many ways..”

Verified user

[Read full review](#) 

Head of Cyber Intelligence at a tech services company with 501-1,000 employees

“I looked at Recorded Future. The main difference is that Cybersixgill is doing one thing, and one thing extremely well, and that is access to Dark Web forums.

Recorded Future was too bloated. It had a lot of additional information that was open source. I don't need that. I get that from other places. I needed something that did one thing and that did it extremely well, and that is access to Dark Web, hard-to-find places, and alerting on infrastructure attacks when mentioned in those places. Recorded Future tries to do the job of two tools. I like the fact that Cybersixgill keeps it separate.

And Cybersixgill was incredibly more affordable than them.

Overall, it was better on several levels:

- focus
- access to specific forums and Dark Web spaces
- simplicity of use; the UI was easier to use and better to look at
- pricing.

Verified user

Lead Cyber Threat-Intelligence Analyst at a educational organization with 10,001+ employees

[Read full review](#) 

ROI

Real user quotes about their ROI:

“If we had to conduct the research that we do with Sixgill ourselves, we would have to hire three or four people to maintain our code and the quality of our CTI service. Sixgill is a significant factor in cutting our costs..”

Verified user

[Read full review](#) 

Manager of Cyber Intelligence Center at a consultancy with 10,001+ employees

“We have seen ROI. It reduces the cost in terms of the number of people that you need to train and have a desk to find the data. It reduced our analysts by half; where we currently have six analysts, we previously needed 12.

It probably reduces our investigation times by an estimated 15 percent..”

Verified user

[Read full review](#) 

General Manager - Cyber Security at a consultancy with 11-50 employees

“It has helped a lot with investigation workloads. In the past, just for one case, we would spend a lot of time sifting through the dark web and tracking back to recognize threat actors. The solution is really helpful because there is no way to search in the dark web. It has saved a lot of time (about 80 percent), especially since we don't have to make sure each site is regulated to meet our intelligence requirements..”

Verified user[Read full review](#) 

Head of Cyber Intelligence at a tech services company with 501-1,000 employees

“I've seen an incredible return on the investment, in the form of time-savings and extremely valuable alerting on infrastructure attacks against us, alerts that I would not have seen if it wasn't for them.

There is also value in our ability to help other organizations that are not as fortunate as we are, organizations that are in our vertical. That has actually put our organization in an extremely good light.

In addition to the reputational, time-savings, and security advantages, there is a cultural advantage, in a way. This is important and is possibly something that we would not think about. It is difficult for large organizations to have patching and addressing of vulnerabilities in an expedited way, when they're dealing with multiple IT departments. But when the threat intelligence team is able to provide the exact time and way in which something is going to be exploited, based on screenshots of forums that detail the targeting, and based on real-life examples of how they do it—the kind of intelligence that we're able to generate because of Sixgill access—it makes patching and addressing of vulnerabilities a lot faster, because it makes them real..”

Verified user[Read full review](#) 

Lead Cyber Threat-Intelligence Analyst at a educational organization with 10,001+ employees

Use Case

“Cybersixgill is a tool that allows you to monitor your organization's exposure to cyber criminals and threats by what I would call scraping Dark Web and underground hacker forum sites.

It's not on-premises. It's a service that's offered by Cybersixgill..”

Verified user

[Read full review](#) 

Lead Cyber Threat-Intelligence Analyst at a educational organization with 10,001+ employees

“We do a heap of open source intelligence collection, where part of that is threat risk assessments for our organization. We use it for being able to conduct searches on Cybersixgill Investigative Portal and identify at risk accounts, current trends, threat data, etc.

We use it as a cloud software as a service provided by Cybersixgill. Therefore, we log into a provided software service, so we are not actually running it on our network..”


Verified user

[Read full review](#) 

General Manager - Cyber Security at a consultancy with 11-50 employees

“We have two use cases. We are providing intelligence and services regarding cyber threats against our clients. Our service covers information from open sources and also the dark web. It's in that context that we are using Sixgill.

For example, we have a credit card issuing company as a client. We use Sixgill to collect information regarding illegal credit card information which is sold on the black market. Sixgill covers many dark web markets, including the dark credit card market as an information source. That means we can easily find our customer's credit card information from Sixgill. We also use their API capability to collect credit card information..”

Verified user[Read full review](#) 


Manager of Cyber Intelligence Center at a consultancy with 10,001+ employees

“We are an MSP who serves different customers of cyber intelligence services. One of the venues that they want to explore is how to do deep web and dark web. For example:

- Is their access for sale?
- Are their analytics for sale?
- Is their monetization for sale?

If there is malware, then this can become a problem for them.

My main use case is using Cybersixgill Investigative Portal as a search engine for anything that happens in the dark web. I also use it for an overall view of the trends regarding malware and bad stuff. It searches to identify the selling of operation or currency information for any of my customers in cyber intelligence services..”

Verified user[Read full review](#) 

Head of Cyber Intelligence at a tech services company with 501-1,000 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.

“In this solution, you only have to give Cybersixgill the email addresses for passes to the platform. It is really simple. You also have two-factor authentication. So, you configure that, and that's it..”

Verified user[Read full review](#) 

Head of Cyber Intelligence at a tech services company with 501-1,000 employees

“The initial setup was straightforward. You just upload the IPs, the domains, and the keywords that you want them to look out for, the ones that are indicative of mentions of your organization, and you're ready to go.

Setting up recurring queries and tracking of threat actors can only happen once you see who's going after you, but the initial setup of the tool can be done within hours.

In our company there are two of us who use the solution, both of us in threat intelligence..”

Verified user[Read full review](#) 

Lead Cyber Threat-Intelligence Analyst at a educational organization with 10,001+ employees

“The initial setup was straightforward. It probably helped that it is SaaS because it was pretty easy. We implemented and started using it the same day.

We knew what we needed. We had seen the product before, so the implementation wasn't too complicated. It was just a case of paying for the license, getting access, and then starting to use it. The tool doesn't need any real training. It is a 20-minute thing, then you are good to go.

I wouldn't see a great deal of benefit trying to deploy it in your own environment because obviously the data is coming from elsewhere. .”

Verified user

[Read full review](#) 

General Manager - Cyber Security at a consultancy with 11-50 employees

“It's a SaaS service, so implementation of Sixgill is not difficult. The deployment didn't take too long. They set it up for us within one week. On our side it was my manager and I who were involved in the setup. And the SaaS means we don't need staff to maintain it. On that side, staff is involved only if we need to contact Sixgill, so one person is enough.

Sixgill has strong capabilities based on search queries, but there is some difficulty in using Sixgill. Their querying is very powerful but it can be difficult. It's not hugely complex but you need some skill to use Sixgill querying.

I have been using Sixgill for more than four years so I know what to expect as the result of the queries, but a beginner might find some difficulty in excluding things from the results and getting what they want. Because Sixgill querying is very flexible, sometimes it returns unexpected results.

We have three staff members using it, all security researchers..”

Verified user

[Read full review](#) 

Manager of Cyber Intelligence Center at a consultancy with 10,001+ employees

Customer Service and Support

“Their technical support was responsive, but they have not achieved a solution yet for the problem that I was having. The issue is that I was having goes beyond just tech support..”

Verified user

Lead Cyber Threat-Intelligence Analyst at a educational organization with 10,001+ employees

[Read full review](#) 

“The technical support is good. The only time that we had a problem, they were very responsive. We have only used them once, which is a good sign of their technical support..”

Verified user

General Manager - Cyber Security at a consultancy with 11-50 employees

[Read full review](#) 

“We use their portal site to get technical support, and Sixgill's customer engagement team frequently provides us with new updates or with important information about our clients. We can also contact them through email..”

Verified user

Manager of Cyber Intelligence Center at a consultancy with 10,001+ employees

[Read full review](#) 

“They have a great team around the platform who are always working to make sure that you receive high value. They ask for feedback all the time. They also listen to the feedback, which is the most important. The CEO company of the company really cares about customer service.

I don't call their technical support because their tool is working properly. If I do have to call Cybersixgill for any reason, they respond immediately..”

Verified user

[Read full review](#) 

Head of Cyber Intelligence at a tech services company with 501-1,000 employees

Other Advice

“We first had to establish what it was we really needed to know. That was very important. Sixgill, Recorded Future, and other CTI platforms provide a lot of information. If we didn't have some specific requirements for this information, we wouldn't be able to find the information that is important to us, in the flood of information.

I would rate Sixgill at eight out of ten. It's a very good solution..”

Verified user

Manager of Cyber Intelligence Center at a consultancy with 10,001+ employees

[Read full review](#) 

“Go for it. It is really simple. If you are unsure that it will give you value, just ask for access for 24 hours. Then, you can explore the solution and see how easy it is to operate it. You will love it. Everybody loves this solution.

The dark web by itself is overrated. Sometimes, you don't find what you want without the context of open sources. I believe Cybersixgill's strongest capability resides with the dark web and deep web. if they go a little into open sources, that is great, but they are good at what they do.

I would rate this solution as 10 out of 10..”

Verified user

Head of Cyber Intelligence at a tech services company with 501-1,000 employees

[Read full review](#) 

“It certainly assists and supports deep, complex investigations. However, in my experience, no tool has complete coverage. If you are talking about deep investigations, then you still need a human to follow up with a lot of the data that Cybersixgill Investigative Portal provides you. It doesn't provide you the answer on its own. As an example, we had a client who had leaked data. Cybersixgill Investigative Portal notified us that that data has been leaked, but it doesn't necessarily tell us the details of what has been leaked. It gives you that prompt, then you need to follow that up with an investigation. Cybersixgill Investigative Portal helps you locate where the data is, but you still need to get the data yourself.

The solution does enable us to do advanced analysis, such as, threat actor profile and social network, but there are limitations to what you can do. It is helpful, but it still needs a trained analyst to make full use of the data that it gives you. I don't think that is a negative thing. That is just the reality of the type of industry that we are in. I don't believe that it's possible to fully automate the advanced analysis.

Eventually, we may increase our usage, but not in the short-term.

Biggest lesson learnt: There are some good tools out there for conducting deep web and darknet investigations.

I would rate this solution as an eight out of 10. It is a good application/tool that makes us more efficient. They are a good team who provide a good service..”

Verified user

General Manager - Cyber Security at a consultancy with 11-50 employees

[Read full review](#) 

“My advice is make sure you schedule a walk-through, and then get it.

I have been very vocal about how much this tool has helped. I'm a big proponent of it. When I talk to people and collaborate with people in other organizations and

they say, "Oh my God, how did you know that?" I'll tell them I knew because of this tool. Others don't do it as well as these people do. This tool does it better than anybody else, because they have focused on one very specific thing and they do it well. Their level of infiltration of these closed forums, and the backend engineering that they've provided, are better than any other solution.

In terms of conducting deep and complex investigations it would depend on how you define those terms. We don't just do threat-actor tracking. Sometimes we're tracking infrastructure and this is not the tool to do that. This is more of an alerting tool. But within the realms and the scope of what Sixgill was created for, you can actually create some pretty advanced tracking queries and alerting. The alerting is invaluable.

For example, by setting queries to track exfiltration of ransomware gangs that employed the double ransom technique, it can exfiltrate the names of any companies that are being ransomed, before they hit the news. That allows me to cross-reference with our third parties and to tell my CSO that a third party is being compromised. I can tell him that before it even hits the news, and that we need to go into protection mode and assume that there might be potential impact to our organization, based on their compromise and the exfiltration of that data..”

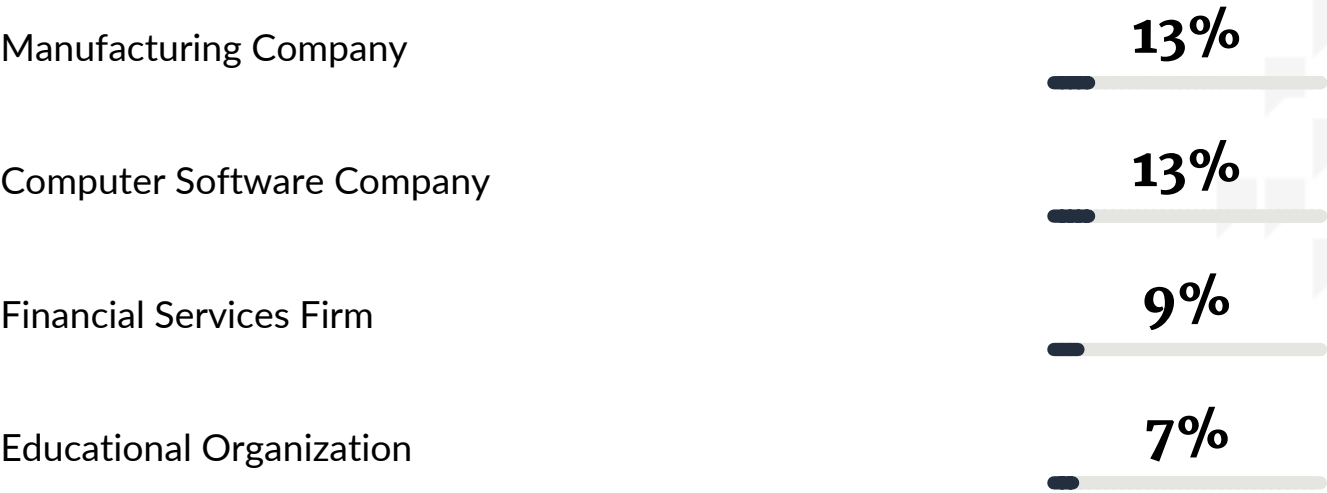
Verified user

Lead Cyber Threat-Intelligence Analyst at a educational organization with 10,001+ employees

[Read full review](#) 

Top Industries

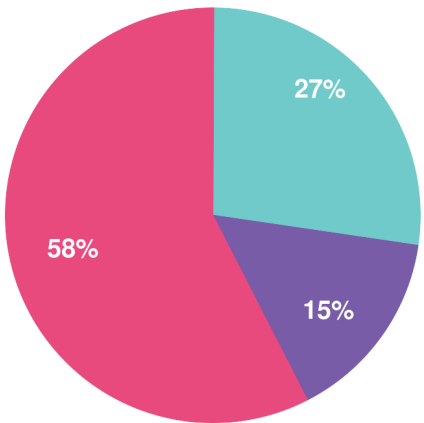
by visitors reading reviews



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 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