



Recorded Future

Reviews, tips, and advice from real users



Powered by  **PeerSpot**

Contents

Product Recap..... 3 - 5

Valuable Features..... 6 - 11

Other Solutions Considered..... 12

ROI..... 13

Use Case..... 14 - 16

Setup..... 17 - 20

Customer Service and Support..... 21 - 23

Other Advice..... 24 - 28

Trends..... 29 - 30

About PeerSpot..... 31 - 32

Product Recap



Recorded Future

Recorded Future Recap

Recorded Future is a powerful and effective cyber threat intelligence (CTI) platform that aims to empower administrators to protect their organizations from threats, both known and unknown. The machine learning engine that Recorded Future utilizes can process the same amount of data that 9,000 analysts working five days a week, eight hours a day for an entire year can process. It simplifies threat detection and remediation so that organizations can focus on other tasks.

Recorded Future Benefits

Some of the ways that organizations can benefit by choosing to deploy Recorded Future include:

- **Quick threat identification and resolution.** The suite of threat detection and resolution features that Recorded Future provides enables users to find and react to threats faster than users who employ their competitors. Organizations can identify 22 times more threats 10 times faster than they would have been able to with any other solution. They can also resolve these threats 63% faster than they were able to before.
- **Access far-reaching deep insights.** Recorded Future gives users the ability to expand their vision beyond that which is immediately visible to them. They can set Recorded Future to detect issues that originate outside of the immediate vicinity of their network. Organizations can utilize machine learning to analyze for links between themselves and the dark web. This provides users insights as to what their vulnerabilities are and gives them insights that they can use to remediate any issues that have arisen or will arise.
- **Customization.** Organizations can integrate Recorded Future with a wide variety of other security tools. If the organization feels that Recorded Future is lacking the capability that they need, then it can expand its toolbox by combining it with other solutions. Additionally, users can easily create dashboards and modify them to best meet their objectives as their needs change.

Recorded Future Features

Some of the many features Recorded Future offers include:

- **Vulnerability scanning tools.** Recorded Future is built with the ability to scan for, identify, and score potential vulnerabilities in real time. It searches a wide variety of sources for information on the risks that an organization faces. This information is analyzed and scored for severity in real time. These tools enable users to prioritize the most severe threats over those issues that will only be nuisances.
- **Threat authentication.** Users can set security protocols that Recorded Future leverages

to reduce false positives. It has tools that compare the detected threats against the organization's protocols. This allows the system to notify administrators whether they are looking at an actual threat or simply a mistake that the system initially misidentified.

- **Attack surface intelligence.** Organizations gain the ability to see the points of vulnerability that would normally be invisible to them and would only be visible to outside attackers. This tool fully exposes the environment that surrounds their network. Everything from historical data going as far back as 10 years to real-time information is gathered so that administrators can create the best possible security strategy for their organization.

Reviews from Real Users

Recorded future is a solution that stands out when compared to its top competitors. Two major advantages it offers are the threat research tools that it provides and the threat monitoring capabilities that it enables users to leverage.

A security operations lead at a comms service provider writes, "Recorded Future covers a lot of different use cases. For example, we are using it for [threat intelligence research](#). We do use the tool to make active research on what is found around the threat. We look at patterns, for example, and see what can be elaborated on from that."

They also write, "We can also use it for [active monitoring](#) in the customer interface. We can monitor the business side of a campaign. We can monitor for specific threats or market activity on the dashboard. We can develop queries to run in a continuous mode in order to get the best reviews."

Valuable Features

Excerpts from real customer reviews on PeerSpot:



“Recorded Future allows me to maintain very accurate alerts.”



Verified user

Head of Cyber Threat Intelligence at a financial services firm with 1,001-5,000 employees



“The solution is diverse and provides me with a lot of different mechanisms for evaluation.”



Dr. Merrick Watchorn

Chief Executive Officer at The Watchorn Innovation Group, Inc. (TWIGI)



“The tool can integrate with a lot of security control and proactive protection devices.”



Verified user

Senior Pre-Sales for Information Security at a computer software company with 51-200 employees



“The intel that they were providing us over the emails was very good. If it found any hashtag in our organization's name on the dark web, a rogue IP, or a marketplace, it would send us an email and notify us that this is being mentioned, and if we want, they can take some action.”



Usman Bhatti

Senior Officer Security Operations Center at a financial services firm with 10,001+ employees



“It can collect data from various sources, including social media and the dark web.”



Bilal Shah

Information Security Analyst at Rewterz



“The tool is helpful in vulnerability assessment of zero-day vulnerabilities and phishing domains. The solution provides information on any domains of the organization that has undergone phishing or any other cyberattacks.”



Pulkit Thakur

Data Engineering Sr Analyst at Accenture



“Has the ability to conduct and build any query without limitations.”



Verified user

Head of Cyber Threat Intelligence at a financial services firm with 1,001-5,000 employees

What users had to say about valuable features:

“Recorded Future has some important strengths. It has a long history of success in the market and is known for excellent threat intelligence. Its team is skilled at using AI to search for and report on threats. For many years, it was seen as the best in the industry..”

Verified user

[Read full review](#) 

Partner, Cyber Security at a financial services firm with 10,001+ employees

“The solution highlights zero-day vulnerability on the world wide web within a short period of time. We get a detailed report on what the vulnerability is all about and whether an expert is available for the vulnerability or not..”

Pulkit Thakur

[Read full review](#) 

Data Engineering Sr Analyst at Accenture

The integration of Recorded Future with my SIEM, specifically Splunk SIEM, has been extremely valuable. Having a layer of intelligence within my SIEM that reflects in Recorded Future, and being able to enrich the data at my SIEM, offers various angles that I wouldn't be able to see without it. Recorded Future allows me to maintain very accurate alerts.

Verified user

[Read full review](#) 

Head of Cyber Threat Intelligence at a financial services firm with 1,001-5,000 employees

“One of the most valuable features of Recorded Future is its ability to detect credential sales on the dark web for websites. It can collect data from various sources, including social media and the dark web. If any suspicious activity is detected, such as the sale of website credentials, I can investigate it and report it to the relevant team. For example, if my domain is sold on the dark web, Recorded Future can detect it.

Recorded Future's threat intelligence platform covers everything from social media to the dark web, allowing for comprehensive recovery and protection of compromised credentials..”

Bilal Shah

[Read full review](#) 

Information Security Analyst at Rewterz

“Recorded Future integrates well with other security solutions in a security stack. It is one of the best things you can spend your money on to obtain better results that are more tailored to your organization.


From the feedback I've received from my clients, the most valuable feature is the ability to personalize the solution. The ability to have a customized dashboard makes it easy for leadership and management to obtain details. Intelligence analysts or security engineers care about the actions and results, whereas the leadership care about graphs and reports. Recorded Future helps my clients create reports and also determine how the intelligence that is generated is consumed. They can easily show the benefits to the leadership without them having to invest 10 hours a week into transferring numbers into a graph or into creating reports..”

Samuel Kotula

Senior Security Consultant at a tech vendor with 201-500 employees

[Read full review](#) 

“Most of the threat intelligence cloud platforms are one-directional solutions, and they just fix the feeds from the cloud, so once they need to build a bidirectional tool, the product should have a third-party tool as a TIF solution or an open-source platform, like OpenCTI, or MISP platform, which is also an open-source platform. The open-source platforms allow Recorded Future to have bidirectional to compare the internal IOCs with the external IOCs and get the common IOCs so that the users can have a good visibility of their internal environment and see what the most APT has targeted in your environment. Recorded Future has developed a browser plug-in that is supported on most browsers, like Google Chrome, Edge, and Mozilla, that allows them to compare the feeds through the different platforms and multi-security control platforms to allow them to compare the threat intelligence feeds and the external feeds through the internal feeds. Once users open any vulnerability management or an SIEM solution and install the plug-ins through the platform or through the browser, so they need to open it through the web console, and the web console will have the bidirectional operation at the end of the the graphic user interface through the client itself through the browser..”

Verified user[Read full review](#) 

Senior Pre-Sales for Information Security at a computer software company
with 51-200 employees

Other Solutions Considered

“Before choosing Recorded Future, we evaluated other options like Mandiant and FortiRecon. We chose Recorded Future because it gives much better results..”

Verified user

Cybersecurity Engineer at a government with 201-500 employees

[Read full review](#) 

“Compared to other tools, Recorded Future's pros are its Intelligence Cards and intuitive graphical user interface. The tool has a plug-in part or the browser plug-in feature. The tool's threat intelligence features could help in comparing the internal feeds with the external feeds, with no need for bidirectional processes. The tool has a one-directional process. What I see with the tool is that it is a very intelligent way to compare the external feed with the internal feed. Most of our clients are complaining about the high false positives of their feeds or the threat intelligence feeds and the expensive subscription activities associated with the tool when I talk about the brand defense or the brand intelligence part of Recorded Future.

ThreatQuotient is a threat intelligence platform, but it doesn't have a commercial feed..”

Verified user

Senior Pre-Sales for Information Security at a computer software company with 51-200 employees

[Read full review](#) 

ROI

Real user quotes about their ROI:

“We haven't seen an ROI. The area that it was used for, as a report, initially was assigned to be used internally only and after that, we decided to try it out as a service to our customers. However, we never sold that service, so we never got a return immediately. .”

Verified user

[Read full review](#) 

Security Operations Lead at a tech vendor with 10,001+ employees

“I believe the commercial feeds or the other niche areas can deliver the return on investment better than Recorded Future. Recorded Future segregates the modules into very few subjects, so it has a huge platform, but in the end, any additional Future should be offered as a different subscription, and you should pay through it. There is no bundle, and no one platform gives you the whole tool..”

Verified user

[Read full review](#) 

Senior Pre-Sales for Information Security at a computer software company with 51-200 employees

Use Case

Recorded Future is my main threat intelligence platform that provides alerts regarding brand protection, relevant threat actors, threat groups, and intelligence vulnerabilities. I use it for research and threat hunting.

Verified user

Head of Cyber Threat Intelligence at a financial services firm with 1,001-5,000 employees

[Read full review](#) 

“We used Recorded Future to find many things like passwords captured in the dark net and websites selling other information regarding our domains. We use the solution to search for our brand or other institutions on the darknet..”

Verified user

Cybersecurity Engineer at a government with 201-500 employees

[Read full review](#) 

“I am working on various alerts related to brand impersonation, typosquatting, abuse domain, and other similar cases. Since the use cases are built-in, I have not created any custom rules..”

Bilal Shah

Information Security Analyst at Rewterz

[Read full review](#) 

“I am currently working with Recorded Future's cloud solution. We provide Recorded Future to our customers as a reseller. We provide the customers with support on the API integration and the bidirectional integration. Mainly, people want the Threat Intelligence Cloud from Recorded Future..”

Verified user

[Read full review](#) 

Senior Pre-Sales for Information Security at a computer software company with 51-200 employees

“As an analyst serving several clients, our team relies on Recorded Future to receive timely alerts related to using underground screen searches. This involves using an algorithmic code feature to gather the specific data we need, which then triggers an alert for us. When we receive the alert on the platform, we assess it to determine if it pertains to our client's needs. If it does, we report our findings to the client..”

Verified user

[Read full review](#) 

Security Analyst at a consultancy with 10,001+ employees

“Being a financial organization, we had a lot of domains, and we were using a lot of public-facing applications. We had listed our public IPs over there, and if any of our licensed applications were found on some sort of dark web or anonymous or rogue IP, or a fake application was being run by using our domain name or using our logo or trademark pictures without authorization, Recorded Future reported it to us.

We were using the cloud service. We were just using it as SaaS..”

Usman Bhatti

Senior Officer Security Operations Center at a financial services firm with 10,001+ 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 was somewhat challenging, and I would rate it between five and six. They need to optimize this process in future updates. While starting with the platform takes a few minutes, seeing real benefits and working efficiently takes a couple of weeks.

Verified user

[Read full review](#) 

Head of Cyber Threat Intelligence at a financial services firm with 1,001-5,000 employees

“I found the initial setup to be easy. On-premises deployments take a few hours, and cloud deployments may take longer. Depending on the client and their level of expertise, the integration of the solution may take a few months to two years. .”

Samuel Kotula

[Read full review](#) 

Senior Security Consultant at a tech vendor with 201-500 employees

“We have it deployed on the cloud. As an analyst, I investigate alerts and escalate them to other teams. I have no idea about integrations, but I find it to be a very friendly tool for a threat intelligence platform..”

Bilal Shah

[Read full review](#) 

Information Security Analyst at Rewterz

“The solution is SaaS-based and deployed over the cloud. The setup is straightforward and everything is available on the tool’s dashboard. We need to provide the tool with the Watch List which contains the company’s name, domain name, or anything that the tool needs to monitor. The tool will report back within one to two days on the Watch List’s update. We can create alerts based on the watches..”

Pulkit Thakur

[Read full review](#) 

Data Engineering Sr Analyst at Accenture

“It was cloud-based, so we didn't have to do too many things on our end. It was just an API connection that we had to do. Our SIEM solution was also integrated with the threat intelligence of Recorded Future. It was pretty handy and easy to configure.

We could implement it in a few days. There were a lot of requirements and queries regarding:

- How will it access our systems?
- Which ports need to be enabled?
- Do we have to go public to expose our network or connectivity?

Sorting these things took time. Overall, it took one to two weeks..”

Usman Bhatti

Senior Officer Security Operations Center at a financial services firm with 10,001+ employees

[Read full review](#) 

“The product's initial setup phase is very intuitive and very easy, as most of the threat intelligence providers, since it can be implemented with API integration.


I believe there's no threat intelligence for on-premises models, but I have worked with two deployments on an on-premises model. The Internet network and other such environments use SaaS products.

The solution is deployed on a hybrid cloud environment because it relies on all the API integrations and interactions with the middleware platform, along with the SaaS platform. The tool doesn't interact with SIEM products directly.

The solution can be deployed in two days. One day is for the implementation, and the second day is for the validation and testing.

I believe the most difficult part in any commercial feeds or threat intelligence feeds is the integration part. If the tool already has some predefined integrations, there is no difficulty. Once you want to integrate a tool with Recorded Future, then for any such new integrations, you should have your API developed or use a third-party firm to operate this process. Everything depends on the complexity of the integrations and the number of resources..”

Verified user

[Read full review](#) 

Senior Pre-Sales for Information Security at a computer software company
with 51-200 employees

Customer Service and Support

The customer support is frustrating and not efficient. They always request logs and screenshots that seem irrelevant. This leads me to avoid using their help desk.

Verified user

Head of Cyber Threat Intelligence at a financial services firm with 1,001-5,000 employees

[Read full review](#) 

“I would rate the technical support a ten out of ten because whenever I have approached them with an issue, they have given me a resolution within 24 hours..”

Pulkit Thakur

Data Engineering Sr Analyst at Accenture

[Read full review](#) 

“The solution has a good technical team. It's part of the package that customers buy into. Each client has an account manager and direct access to live customer support. The team responds fast. .”

Verified user


Partner, Cyber Security at a financial services firm with 10,001+ employees

[Read full review](#) 

“I had a direct line to the technical support team when I was working at the organization. They had a technology portfolio and I was on the board. They spent a lot of time explaining how the technology works, which is why they were selected by US CyberCom as they had made a strategic investment in making sure they could explain their software. .”

Dr. Merrick Watchorn

Chief Executive Officer at The Watchorn Innovation Group, Inc. (TWIGI)

[Read full review](#) 

“We faced some difficulties initially due to our unfamiliarity with the tool. However, after reaching out to their tech support team, we received excellent assistance from their cooperative staff. With their help, we were able to resolve our issues quickly and efficiently. However, there have been some times when the knowledge of the agent could have been better.

I rate the support of Recorded Future an eight out of ten..”

Verified user

Security Analyst at a consultancy with 10,001+ employees

[Read full review](#) 

“In one instance, we had to get their technical team on board for justification and explanation of things that we couldn't understand. It was regarding the intel provided on the images and the trademarks of our organizations. A lot of fake pages and posts were being posted using our trademark, pictures, etc. We took it up with their technical team, and they told us how things are working and how the AI is working to correlate our data.

I'd rate them a nine out of ten because most of the time, as soon as we raise any case or have any queries, they get back within hours or minutes..”

Usman Bhatti

Senior Officer Security Operations Center at a financial services firm with 10,001+ employees

[Read full review](#) 

Other Advice

“Recorded Future is a great tool overall for threat intelligence. I think it's one of the best to add to an organization's security stack. However, the licensing costs are extremely high for small- to medium-sized companies. As such, I would rate it at nine on a scale from one to ten, with one being the worst and ten being the best..”

Samuel Kotula

Senior Security Consultant at a tech vendor with 201-500 employees

[Read full review](#) 

“Organizations must have at least two dedicated technicians working with the solution since the learning curve is a little big. To use the solution to its maximum capacity for the first year, having at least two technicians working with Recorded Future is better.

Overall, I rate Recorded Future ten out of ten..”

Verified user

Cybersecurity Engineer at a government with 201-500 employees

[Read full review](#) 

“Recorded Future covers the whole area of social media in terms of threat detection. I would suggest it to everyone as it is a very user-friendly platform that detects all things related to your domain, from the dark web to social media.

Overall, I would rate the solution an eight out of ten..”

Bilal Shah

Information Security Analyst at Rewterz

[Read full review](#) 

“Go for it because of the features they are offering. They are quite competitive in the market. Along with the basic features, you can also get specific features you want. For example, we took the takedowns and watchlist services. It's a good product.

I have not worked with other paid threat intelligence platforms. I have used the public ones though. It offers great value for your money, and there are also notifications and things like that. They offer quite good services.

Overall, I'd rate it an eight out of ten. .”

Usman Bhatti

Senior Officer Security Operations Center at a financial services firm with 10,001+ employees

[Read full review](#) 

“I'd still recommend Recorded Future for large organizations, but they must understand the business model and pricing. The quality of Recorded Future, Mandiant, and CrowdStrike seems quite similar, though I'm not a deep technical expert. The choice depends on the customer's needs – not all customers need every

feature.

I can't definitively say which is better regarding AI technology as I haven't technically compared them myself. The solution might be advantageous due to their extensive experience in the area. However, with Google's resources behind Mandiant, they likely have significant capabilities, too. Google's resources are probably on par with Microsoft's, so they could easily ramp up their technology if needed.


When discussing AI in these threat intelligence setups, clarifying what we mean is important. Often, it's a system of rules analyzing abnormalities and triggering actions. I frequently ask what people mean by AI in different contexts because it often comes down to rules: if certain events occur or parameters are exceeded, what actions should be taken? These systems analyze data in real-time and feed it to the Security Operations Center to create a more efficient setup with fewer false positives.

False positives are a major challenge, especially for smaller companies. If they don't have well-trained IT staff, dealing with numerous false positives can be more trouble than it's worth. I've seen smaller organizations struggle with this – sometimes, it's almost better for them not to have these systems if they can't understand and manage them effectively.

I rate the overall product as nine out of ten. .”

Verified user

Partner, Cyber Security at a financial services firm with 10,001+ employees

[Read full review](#) 

“There are two parts to the daily cybersecurity operations. There are two types of customers. Some customers already have solutions that can handle multi-commercial threat intelligence feeds, and the other clients don't have any threat

intelligence platform, so they just depend on one threat intelligence commercial feed. The second type of customers can use Recorded Future as a TIF provider. They can integrate the platform with all of their security through the plug-ins and the API integrations offered by the product.

Speaking about the real-time analysis feature of Recorded Future impacting the incident response time, I would say that the tool has an interactive portal. What I mean by the interactive portal is that there are many other threat intelligence fields. The tool gives or provides you with a fixed report, so you can't segregate or delegate some parts of the report to other teams or to a malware analysis team to segregate the duty. There is no segregation possible through the tool's reports. What is unique in Recorded Future is that it can segregate the threat intelligence activity and the threat activity or the threat hunting activity through many teams, such as the malware analysis team with its business intelligence feature. The tool has something called Intelligence Cards, which allows the product to give users more details through any IOC provided.

I have SecDevOps-driven cybersecurity strategies that are supported by Recorded Future. The tool can integrate with a lot of security control and proactive protection devices.

I believe the tool's maintenance depends on the OS users work with, meaning it all relies on the operation system that handles the integrations. Maintaining the tool is unnecessary, as it is a straightforward platform.

My recommendation of the tool to others depends on their use cases. If someone has a lot of enterprise-level skills and teams, such as threat intelligence teams, IR teams, and malware analysis teams, then Recorder Future will facilitate processes like threat enrichment and threat sharing among those teams. For those who are looking for accuracy and to get the right feeds for their investigation, I would not recommend using Recorded Future because there are so many unknown or niche cybersecurity platforms in the market that have more visibility and more accuracy in the area of commercial feeds because I believe such products use the human resources to validate those feeds. Recorded Future doesn't have the capability to validate its feeds. The tool relies on its own algorithm and the government's feeds for the threat intelligence feed. Even with Recorded Future, some of our clients

didn't have an IR team to validate their activities to filter the most accurate feeds and avoid noisy feeds.

I rate the tool a seven out of ten..”

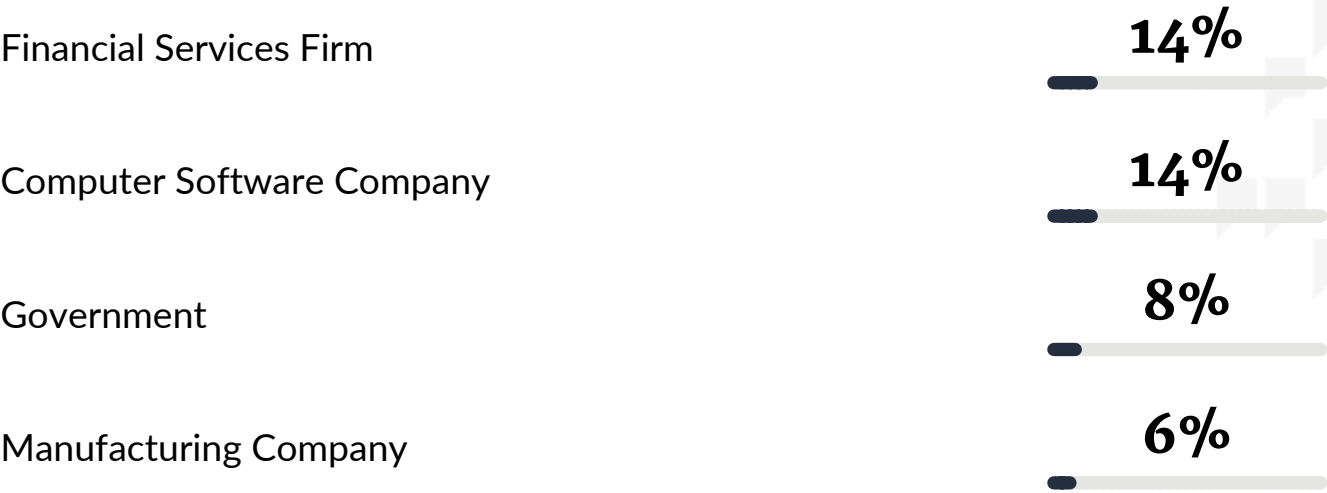
Verified user

Senior Pre-Sales for Information Security at a computer software company with 51-200 employees

[Read full review](#) 

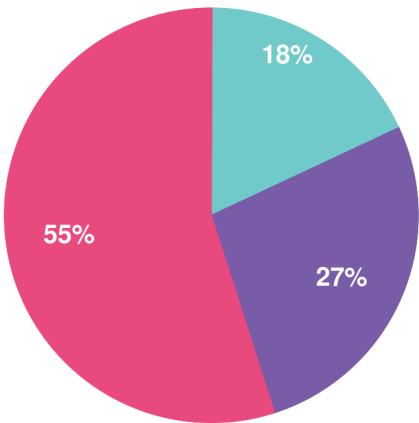
Top Industries

by visitors reading reviews

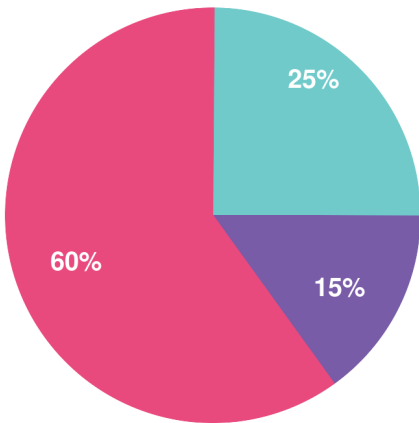


Company Size

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 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