aws marketplace

MetaDefender

Reviews, tips, and advice from real users






Powered by PeerSpot

Contents

Product Recap

MetaDefender

MetaDefender Recap

MetaDefender offers a robust cybersecurity platform focused on data protection and threat detection designed for organizations seeking advanced security measures.

MetaDefender enhances security through multi-scanning and file-based threat prevention. It provides rapid detection to safeguard data and systems effectively. Its multi-faceted approach ensures comprehensive coverage, accommodating the needs of tech-savvy businesses. Recognized as a reliable choice in cybersecurity, it meets industry demands with its innovative solutions.

What features define MetaDefender?

- Multi-Scanning: Utilizes multiple antivirus engines for enhanced threat detection.
- Data Sanitization: Removes potential threats while retaining file usability.
- File-based Threat Prevention: Detects and neutralizes attacks within files.
- Advanced Threat Protection: Safeguards against zero-day vulnerabilities.

How does MetaDefender benefit organizations?

- Increased Security: Strengthened protection against cyber threats.
- Operational Efficiency: Reduces downtime with efficient threat management.
- Regulatory Compliance: Aids in meeting industry compliance standards.
- Reduced Risk: Minimizes potential data breaches.

MetaDefender is extensively implemented in industries such as finance and healthcare, where data protection is critical. Its ability to seamlessly integrate with existing IT infrastructure makes it a preferred choice for organizations requiring tailored cybersecurity solutions without compromising operational workflows.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- "MetaDefender is 100% stable, making it one of the best cybersecurity solutions we offer, which provides confidence in promoting and recommending it to others."

Verified user

Partner Account manager at a wholesaler/distributor with 51-200 employees

- "OPSWAT is the best alternative."

Eido Ben Noun

Cyber Security Architect at Diffiesec

- "Overall, MetaDefender is a strong solution for file security, especially for handling email attachments and downloadable files."

Pavan Ingaleshwar

Soc Analyst at a consultancy with 11-50 employees

"MetaDefender has positively impacted my organization by reducing the risk of file-based attacks, which has significantly improved our overall defense against phishing and malware delivery techniques."

Salbu Kumar

Manager at Cyvogenix

"The best feature of MetaDefender is that it can isolate USB devices from the connected network, blocks malware and unsafe files, and ensures all endpoints follow security policy, so that my organization remains safe and reduces the risk of these threats."

Islam Hamada

Network Security Engineer at EMAK For Integrated solutions

"For one of my clients, a major bank in Turkey, they reported saving approximately 30 percent of their SOC time on analyzing emails since implementing MetaDefender."

Dincer Oksuzbakan

Cybersecurity Architect at Natica IT Consulting

"I like the simplicity, the way it works out of the box. It's pretty easy to run and configure. The integration of the network devices with the ICAP server was easily done."

Verified user

Cyber Security Specialist at a insurance company with 1,001-5,000 employees

What users had to say about valuable features:

“MetaDefender offers some of the best features such as multiple engine malware scanning, content disarm and reconstruction (CDR), deep file inspection, and strong API-based integrations. Deep file inspection is the feature I find myself using the most, as it helps in my workflow significantly. The multi-engine approach gives more confidence compared to relying on a single antivirus engine, especially for zero-day threats.

MetaDefender's effectiveness in blocking or sanitizing content based on policy is very strong. A combination of multi-engine scanning and CDR makes a big difference. It does not just rely on a signature; it enforces policy at the file level. Policies like blocking files with high-risk indicators, sanitizing documents with embedded macros, and allowing only clean files into the environment show its strengths. MetaDefender is very effective in sanitizing files without breaking usability. The integration of multi-scanning and Content Disarm and Reconstruction affects our data security operations. MetaDefender plays a very important role in today's threat landscape, which heavily uses documents and file-based payloads..”

Salbu Kumar
Manager at Cyvogenix

Read full review

"The best features of MetaDefender include strong sandbox analysis, file reputation, threat intelligence, and data sanitization, which removes hidden threats from files and provides better confidence during investigations. Rather than relying on a single antivirus engine, MetaDefender checks files using multiple engines, which truly helps.

I find myself relying most on sandbox analysis and file reputation, which are two features I genuinely appreciate from this tool. The sandbox analysis, file reputation, and threat intelligence stand out as key features.

MetaDefender positively impacts the organization by reducing the risk of malware entering our security environment, providing faster file analysis during incidents, and improving our confidence when handling suspicious attachments. Sometimes, files that traditional scanners deem safe may contain malicious elements, so using MetaDefender gives us the assurance we need when investigating malware or attachments.

The Deep CDR feature effectively removes risky content and rebuilds safe files, neutralizing even unknown threats. Unlike signature-based detection that only addresses known threats, CDR works by eliminating suspicious content, making it superior in practical scenarios where files such as PDFs and Office documents can be safely delivered to users without risk while maintaining usability.."

Pavan Ingaleshwar
Soc Analyst at a consultancy with 11-50 employees

Read full review

"The detection rate of the MetaScan multi-scanning feature is very high. When discussing Linux with five engines or ten engines, it can detect most of the viruses that are tested. I have seen very few instances where customers reported a virus that was not blocked after a PT scan. When we verify these cases, we confirm they occurred. Of course, every engine has its own detection rate, and you cannot achieve 100 percent detection. When using MetaDefender especially on Windows, the detection rate is very high, and it increases as you use more engines. Most customers I see using eight or twelve engines on Windows have good results with both configurations. When customers use a large number of engines, such as twenty engines with integration to external scanners, the results look almost perfect because in cyber security, there is no 100 percent, but it is close to that.

The effectiveness of Deep CDR in reconstructing files safely and without signatures is very effective. When people configure Deep CDR correctly, it performs as it should. Sometimes some files are negatively affected by CDR. If I must be specific about what could be helpful, it would be to create a policy or workflow in OPSWAT terminology that handles cases when CDR cannot be performed or harms the file. I am not certain if the system can check whether CDR has harmed a file, but I know of use cases where CDR was disabled because it made files unable to open or unable to open properly. I believe this is very effective and is the most effective engine of OPSWAT because customers ask for OPSWAT for two main reasons: the CDR capabilities and the multi-scanning engines.."

Eido Ben Noun
Cyber Security Architect at Diffiesec

Read full review

"In my experience, the best features MetaDefender offers include the number of different antivirus engines that can scan files through multi-file scanning, often using 20 to 30 engines, with the top premium package around 33 engines, capturing 80 to 90% of malware in all those files. If any engine detects malware, the file is blocked, which increases detection because different engines catch different malware.

When dealing with central government and defense, we find that if there is any kind of malware on the network or the file, whether that is a software file, hard disk file, or a pen drive, it cannot be allowed on the network. This is when we put it into the sandbox and perform file sanitization to ensure that nothing malicious comes into the network.

Whenever we are dealing with central government or defense contracts, MetaDefender's core philosophy of trusting no file means it scans files, rebuilds them, and verifies their reputation, ensuring they contain no malicious content. This positively impacts our organization by detecting malware and stopping any kind of data leaks through the network.

In terms of measurable outcomes across central government and defense, we are seeing saved time when files go through the antivirus file scanners. In financial services, such as with mortgage applications, the process sends files straight into MetaDefender file scanning that cleans out any malicious content.."

Verified user

Partner Account manager at a wholesaler/distributor with 51-200 employees

Read full review

“The best features MetaDefender offers include its Content Disarm and Reconstruction, which is a key feature chosen by our clients because many other products claim to provide that functionality, but generally, they cannot do it as cleanly. Through Proof of Concept sessions with our clients and the OPSWAT team, they see that MetaDefender's Content Disarm and Reconstruction is strong, usable, and valuable for our customers, making them want to work with OPSWAT specifically for this feature.

“For example, one of our customers was not using any Content Disarm and Reconstruction technology but was receiving emails containing PDF documents or XLSX documents, some with malicious content. MetaDefender's technology worked effectively, disarming and reconstructing PDFs to deliver clean copies to their users, while allowing their analysts to see the malicious code.

“MetaDefender has positively impacted my clients' organizations by saving time for their SOC teams who were previously receiving false positives and unnecessary alarms from other products, allowing them to focus on analyzing real threats, which has led to fewer incidents.

“For one of my clients, a major bank in Turkey, they reported saving approximately 30 percent of their SOC time on analyzing emails since implementing MetaDefender.

“MetaScan multi-scanning feature is excellent because it provides multiple vendors for scanning. If one vendor fails, the others remain operational, ensuring continued protection.

“Assessing the effectiveness of Deep Content Disarm and Reconstruction in reconstructing files safely and without signatures reveals it to be effective, as clients receive identical documents without changes other than the removal of malicious code.

“MetaDefender's file-based vulnerability assessment analyzes binaries and installers for known vulnerabilities before they enter a network, providing a proactive defense that is highly valuable for our customers..”

Dincer Oksuzbakan
Cybersecurity Architect at Natica IT Consulting

Read full review

"The best feature of MetaDefender is that it can isolate USB devices from the connected network, blocks malware and unsafe files, and ensures all endpoints follow security policy, so that my organization remains safe and reduces the risk of these threats.

"I find MetaDefender effective when it comes to blocking or sanitizing content based on the policies in place because it removes hidden threats and scans devices and endpoints, protecting the environment against unknown and advanced attacks.

"The integration of Multi-Scanning and Content Disarm and Reconstruction affects my data security operations positively as it is easy to integrate into my environment.

"I find the multi-scanning mechanism and content disarm and reconstruction features beneficial for data security, as MetaDefender's endpoint creates a secure layer to protect my organization from threats and attacks.

"The main benefits that MetaDefender brings include isolating USB devices from attacks, removing hidden threats such as malware and malicious attacks, and protecting against unknown and advanced attacks.

"My impression of the detection rates provided by MetaScan Multi-Scanning is that they are good, as the scanning of MetaDefender removes hidden threats, detects known issues, and protects devices from unknown malware and attacks.

"I assess the effectiveness of Deep CDR in reconstructing files safely without signatures. CDR used in MetaDefender effectively removes dangerous and unsafe attacks by taking a file, removing risky parts, and delivering a clean version to the user, as it removes scripts, hidden links, and malicious components.

"I use Adaptive Sandbox Analysis and a sandbox to detect advanced threats, as it receives files, runs them in a VM environment, and discovers the behavior of these files, allowing safe files to return while blocking any that behave poorly.

"I find that the features of MetaDefender are strong, and its work is effective for scanning and securing the environment from malware and operates well.."

Islam Hamada

Read full review

Other Solutions Considered

"We have not used a different solution. We focus on best-in-breed vendors, with Opswat being our chosen solution due to its effectiveness in the market.."

Verified user

Partner Account manager at a wholesaler/distributor with 51-200 employees

Read full review

"Previously, we used traditional antivirus solutions that utilized only single engines, which is why we switched to MetaDefender, as it offers numerous features and capabilities that are advanced compared to traditional antivirus solutions.."

Pavan Ingaleshwar

Soc Analyst at a consultancy with 11-50 employees

Read full review

"Before choosing MetaDefender, we considered alternatives such as Reversing Labs but found their offerings to be inferior, especially for our defense and central government contracts, where Opswat stands out as far superior.."

Verified user

Partner Account manager at a wholesaler/distributor with 51-200 employees

Read full review

"Before choosing MetaDefender, we evaluated basic antivirus and file scanning solutions that were already part of our environment. These tools only provided single-engine detection and were limited in their coverage and advanced features such as multi-engine scanning and CDR. MetaDefender was ultimately selected for its comprehensive approach that combines multiple antivirus engines and sandbox analysis with file sanitization.."

Pavan Ingaleshwar
Soc Analyst at a consultancy with 11-50 employees

Read full review

"I decided to switch to MetaDefender because Kaspersky could only detect malware but not take action, whereas MetaDefender detects and prevents threats simultaneously.

"I chose MetaDefender because it is capable of adding multi-layered security that prevents threat detection and removes unknown threats, working without signature-based detection, which is beneficial.."

Islam Hamada
Network Security Engineer at EMAK For Integrated solutions

Read full review

"I have used alternatives to MetaDefender, but not as an administrator, only as a user. I used some kiosk products similar to MetaDefender kiosk. There is an alternative called Sasa Software, I believe it is Sasa Scanner or Gateway Scanner. I used it, but the user interface is not as good as OPSWAT. The experience with this product is not as good as the experience with OPSWAT, and the time it took to scan some large files was very long. OPSWAT is the best alternative. I also see on customers' side another product called RESEC, and this product also was not a good experience. The user experience is not good enough in this field, and when users try to configure policies, it lacks features when compared to OPSWAT.."

Eido Ben Noun
Cyber Security Architect at Diffiesec

Read full review

ROI

Real user quotes about their ROI:

"I have not seen a direct return on investment, but clients have noted that the product saves time and may reduce the need for fewer employees since the SOC team focuses on critical incidents as MetaDefender handles current analyses efficiently.."

Dincer Oksuzbakan
Cybersecurity Architect at Natica IT Consulting

Read full review

"We see a return on investment as MetaDefender prevents malware incidents, saves investigation time for SOC analysts, and reduces the overall impact of threats. This indirectly saves costs and efforts for organizations that implement it.."

Pavan Ingaleshwar
Soc Analyst at a consultancy with 11-50 employees

Read full review

"I believe it is worth the money, as it brings time-saving, cost-saving, and efficiency improvements, especially in large environments. However, in smaller environments, it incurs high costs. Overall, it is good because it has many features for scanning and cleaning the environment from malware and saves time.."

Islam Hamada
Network Security Engineer at EMAK For Integrated solutions

Read full review

"MetaDefender has positively impacted my organization by reducing the risk of file-based attacks, which has significantly improved our overall defense against phishing and malware delivery techniques. We have seen around a 40% drop in malicious file incidents, and our SOC team is spending less time on manual file analysis now.."

Salbu Kumar
Manager at Cyvogenix

Read full review

"I believe we see a return on investment through time savings and reduced need for unnecessary personnel. Having both cloud and on-premise solutions enables effective file sanitization and vulnerability detection while preventing attacks that save costs and protect reputation.."

Verified user
Partner Account manager at a wholesaler/distributor with 51-200 employees

Read full review

Use Case

“The use cases for MetaDefender involve checking an endpoint, such as a laptop or USB, to ensure that they are safe, clean, and meet security policy before they connect to the network. I can use it for malware and unknown devices' security status..”

Islam Hamada
Network Security Engineer at EMAK For Integrated solutions

Read full review

“MetaDefender is used in one of our client environments where every file upload to their web portal goes through the scanning process. It scans using multiple engines and applies CDR before allowing the file into the system. This has helped us stop suspicious documents even before users interface with them.

With the increase in phishing and document-based attacks recently, this kind of file sanitization layer has become very important for us..”

Salbu Kumar
Manager at Cyvogenix

Read full review

"I deploy it in different environments and manage a team of professional services that deploy MetaDefender products in customer environments. I talk with customers and am aware of use cases where new or additional needs arose after MetaDefender deployment. For example, customers needed to transfer files between source and destination using MetaDefender. I know that MetaDefender File Transfer Protocol, or MFT, is now supported, but in the past, it was not. There are products that have been developed from customer needs, such as products that can transfer files from source to destination with integration to MetaDefender.."

Eido Ben Noun
Cyber Security Architect at Diffiesec

Read full review

"MetaDefender serves as a file security gateway that scans, cleans, and sanitizes files before they are allowed on the network, which stops malware, ransomware, zero-day attacks, and any kind of malicious files from entering the network.

For one of our partners, we were dealing with a large financial services business handling mortgage applications. When files were scanned into the network, every single file that was sent was then scanned by the multi-scanner, and if any contained even a slight amount of malware, we performed deep CDR file sanitization that removed everything that could be malicious and rebuilt the file.

The main use cases that we tend to see are all the antivirus engines as part of the multi-scan, and the second use case that is emerging frequently is file sanitization, also known as deep CDR.."

Verified user
Partner Account manager at a wholesaler/distributor with 51-200 employees

Read full review

"I primarily use it for file security and malware analysis, helping me scan files, detect threats, and validate suspicious attachments before they reach end users. The multi-engine scanning and sandbox analysis provide an extra layer of security to the environment, ultimately improving detection capability and reducing the risk of malware infection.

One instance involved a user receiving a suspicious email attachment that appeared normal, but MetaDefender flagged it through one of its engines, leading to a deep analysis that revealed it was malicious. This helped us block the file before it reached end users.

Another important use case is that it helps us scan email attachments and downloadable files using its sandbox capability, detecting malware with multiple antivirus engines and validating suspicious files during investigations. As a SOC team, whenever we receive a suspicious file or alert, we use MetaDefender to analyze it before taking any action.."

Pavan Ingaleshwar
Soc Analyst at a consultancy with 11-50 employees

Read full review

“My main use case for MetaDefender is for our client's environment, which is using MetaDefender for their OT security or for their email side. All clients use MetaDefender, and it is especially great for Content Disarm and Reconstruction, which they want to leverage.

“For example, one of our clients is using MetaDefender for their email gateway site as their mail gateways, scanning emails. Generally, they use MetaDefender's Content Disarm and Reconstruction property for that email scanning.

“None of my customers are using the reporting and audit visibility features on MetaDefender platform.

“Integrating multi-scanning and Content Disarm and Reconstruction positively affects my clients' data security operations, prioritizing security over potential delays experienced by end users..”

Dincer Oksuzbakan
Cybersecurity Architect at Natica IT Consulting

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 deployment of MetaDefender on Windows and Linux machines is very easy and quick. When discussing deployment of containers or deployment in Kubernetes environments, it sometimes takes too long. The deployment of the sandbox product takes too long. The deployment of MetaDefender email security, core, and MetaDefender kiosk has very easy and quick deployment.."

Eido Ben Noun

Cyber Security Architect at Diffiesec

Read full review

“The implementation was straightforward. MetaDefender is quite easy to use. Installing it is very simple. The basic concepts are easy to understand.

We spent about two weeks implementing and configuring this. We wrote custom libraries with some scripts, and that's all. And it has been running for two years so far. We enabled automatic updates and it just works.

We have it deployed fully on-prem because we have sensitive data. We have it in two separate data centers. One is in Warsaw and the second is in Krakow.

There is no maintenance involved..”

Verified user

Cyber Security Specialist at a insurance company with 1,001-5,000 employees

Read full review

Customer Service and Support

“The support is good, really responsive. They usually respond within two hours or less, and we fix issues in about two days.

There is a guy there named Vlad. He is a great technician who has helped me many times when I had trouble with licenses or questions on how to do something differently. The support is great..”

Verified user

Cyber Security Specialist at a insurance company with 1,001-5,000 employees

Read full review

“Customer support from Opswat is commendable. Their customer service team, distribution team, and regional sales managers provide excellent aftercare and set us up for upselling across the entire MetaDefender portfolio.

From a partner's perspective, the channel team and customer service have delivered strong support. I would rate it a nine because I have not interacted with customer support directly, though the support provided has been strong..”

Verified user

Partner Account manager at a wholesaler/distributor with 51-200 employees

Read full review

"I have contacted the technical support of OPSWAT. The quality of answers from support has been very good most of the time. It can be useful when contacting support to mention what needs to be collected and what needs to be sent before opening the ticket. For example, if discussing an issue, support will probably ask for specific logs. This can save time because many vendors, when they check something and ask for logs, need those logs from the beginning. If you open a ticket and the answer is to proceed, and the answer after one day is that specific logs are needed, it is better to know that from the beginning.."

Eido Ben Noun
Cyber Security Architect at Diffiesec

Read full review

Other Advice

"I recommend MetaDefender to others because it is effective, has high stability, and is beneficial for environments. I have rated this review a ten out of ten.."

Islam Hamada
Network Security Engineer at EMAK For Integrated solutions

Read full review

"I would do a proof of concept because we are talking about cybersecurity. We ran tests for free for about three months. After our testing we were happy with the results.."

Verified user
Cyber Security Specialist at a insurance company with 1,001-5,000 employees

Read full review

"To achieve a perfect score of 10, MetaDefender would need to cater to every partner's ability to sell. While the price is a consideration, the benefits of scanning, removing, detecting, and sandboxing outweigh it significantly.

I advise those considering MetaDefender to reach out to reseller partners for guidance on file sanitization and to explore setting up a proof of concept to see the value MetaDefender brings, with demos available directly on their website.

My overall rating for this solution is 9.."

Verified user
Partner Account manager at a wholesaler/distributor with 51-200 employees

Read full review

"MetaDefender is a very time-saving and effort-saving tool. I advise others looking into using MetaDefender to understand their file flow properly before deployment. If integrated correctly, it becomes a very strong layer against modern file-based attacks.

"Threats in a file are cleaned before they reach the core, creating a silent shield in place. The SOC workload has reduced because fewer suspicious files reach analysis, and users do not complain much since files still open normally after sanitization. I would rate this review an 8.."

Salbu Kumar
Manager at Cyvogenix

Read full review

"The file-based vulnerability assessment feature in MetaDefender is very valuable for identifying vulnerabilities before deployment, especially in environments

where files or applications are frequently shared. It detects outdated components, known vulnerabilities, or risky configurations within files prior to execution, which is essential since many vulnerabilities arise from outdated libraries or insecure files. From a SOC perspective, this feature offers a proactive layer of security, enabling teams to identify and fix issues before they escalate into incidents.

We use the audit visibility feature in MetaDefender, which helps during audits by providing reports that demonstrate which files were scanned and what threats were identified. This is particularly useful when explaining our security protocols to client-side technicians. For example, during an audit, we can show the report of scanned files as proof that our security checks are in place.

From my experience, MetaDefender is quite effective in blocking and sanitizing content based on defined policies, allowing organizations to set rules for file handling such as blocking high-risk files and sanitizing them with CDR before delivery. This is crucial because it ensures that even if files contain hidden threats, they can be reconstructed safely for sharing. For the SOC, this minimizes the risk of malware reaching end users and allows for flexibility in fine-tuning policies based on our security environment. In practice, it automates decision-making, reducing the need for manual analysis and enforcing strong security policies.

For organizations dealing with email attachments and file uploads or downloads, my advice is that MetaDefender is a very useful tool as it adds an extra security layer and assists SOC teams in validating threats more confidently.

During my use, I have not observed any major downtime or performance issues. Overall, MetaDefender is a strong solution for file security, especially for handling email attachments and downloadable files. The multi-engine scan and CDR feature provide an extra layer of protection, effectively preventing both known and unknown threats. I would rate this solution an eight out of ten overall.."

Pavan Ingaleshwar
Soc Analyst at a consultancy with 11-50 employees

Read full review

“The sandbox helps in cases of suspicious files. However, the sandbox alert indicates suspicious activity for many different files. When we test some files that we download from vendors' official sites for server BIOS upgrades or firmware upgrades on servers, such as files from Dell or HPE, these files are also considered suspicious for many use cases. The sandbox is good only for specific areas. If discussing email, it can be good. However, if discussing large files, the sandbox can indicate suspicious activity in almost every executable file. This causes customers not to believe in the results. They say it is suspicious, but it is fine to them. Even if something is actually suspicious, it does not receive attention because of the many files that should be legitimate but are considered suspicious.

Perhaps the effectiveness of the sandbox and level of suspicious files can have two different levels. If asked how it can be better, a different score or different tag for suspicious files from known vendors and suspicious files from unknown vendors could help. Multiple levels of suspicious files, scores, or tags could be something that can be configured. For example, when using the sandbox to scan files that you download from the internet to different environments, such as air gap environments, and in this environment you manage IBM servers, if you scan the file and select that you are using it for IBM servers before scanning, it could be considered less suspicious. The system could also load a certificate of the file that you download and then determine whether it has a trusted certificate or a certificate that is probably good enough or probably not suspicious most of the time.

I am not certain if MetaDefender can do anything else. Perhaps if they want to improve vulnerability management, instead of managing static CVEs, they could have a different method involving CVEs but something else as well. For example, CVEs that can be harmful because they are exploitable could be differentiated. However, this is something that cannot be managed at the MetaDefender level because it is just about files on a perimeter and does not understand the deployment of the environment because it is not running in the real environment. I am not certain if there is a way to do this better.

There are some upgrades when MetaDefender has new features, so you have to

upgrade. This is not about the upgrade of the engines that happen all the time if you have an internet connection or do it manually. The maintenance can take significant effort that causes most people not to upgrade and update it all the time. Considering offline users, offline environments, and environments with no internet, easier updates could be helpful. The upgrade of MetaDefender version, whether email or MetaDefender Core, is very quick. I would rate this review eight out of ten.."

Eido Ben Noun
Cyber Security Architect at Diffiesec

Read full review

Top Industries

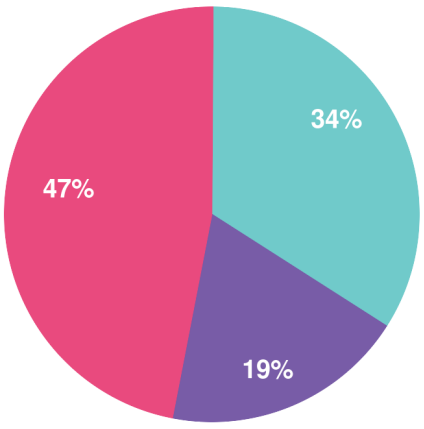
by visitors reading reviews

Financial Services Firm	14%
Computer Software Company	13%
Healthcare Company	10%
Construction Company	8%

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