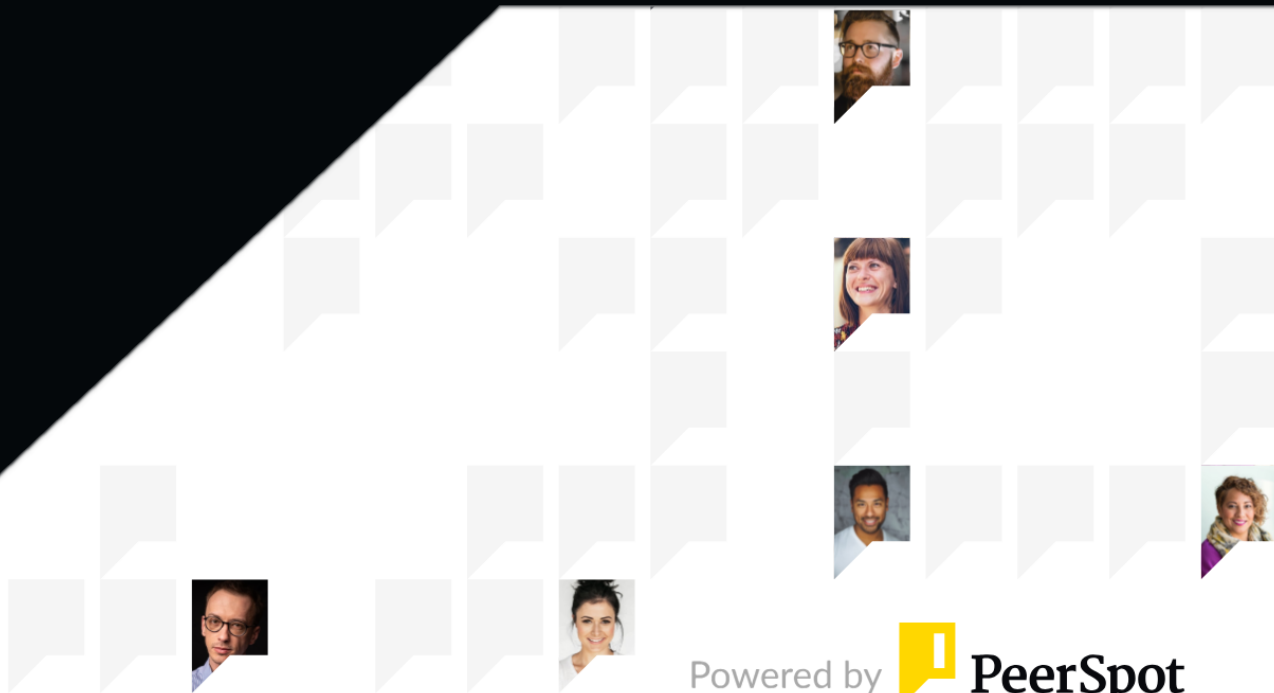


aws marketplace

MetaDefender

**Reviews, tips, and
advice from real users**



Powered by  **PeerSpot**

Contents

Product Recap..... 3 - 4

Valuable Features..... 5 - 12

Other Solutions Considered..... 13 - 14

ROI..... 15 - 17

Use Case..... 18 - 21

Setup..... 22 - 24

Customer Service and Support..... 25 - 27

Other Advice..... 28 - 33

Trends..... 34 - 35

About PeerSpot..... 36 - 37

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 a useful tool for scanning all incoming and outgoing files and keeping our applications and servers in compliance, and I found it useful because we can integrate it with multiple file transfer tools such as Globalscape EFT, GoAnywhere, or Sterling, which is the best feature as it integrates with multiple tools.”



Ravi Raushan Singh

Senior Associate at a educational organization with 11-50 employees

- ✓ “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



“MetaDefender OPSWAT provides that solution, and also the ICAP scans.”



Kevin-Liu

Information Security Consultant at a tech vendor with 51-200 employees



“The percentage of accuracy is great and the integration of multi-scanning and Content Disarm and Reconstruction affects my data security operations effectively because OPSWAT blocks the file types that we are not willing to have inside the company or are not approved.”



Denis Burnaev

Infrastructure Security & Cyber Engineer at El Al



“I assess the effectiveness of MetaDefender in blocking or sanitizing content based on policy as very good.”



Alex Nigai

Integration Technician at danet



“MetaDefender is leading with respect to competitors as an all-in-one platform because no other tool has all the platform built-in.”



JaiminDalwadi

Delivery Lead at altisec

What users had to say about valuable features:

“The best features MetaDefender offers are the ICAP Scan and API Scan. For the ICAP Scan and API Scan, they stand out to me because they are easy to manage and can also adopt multi-clients at the same time and scan by seven different scan engines and different antivirus signatures scan.

MetaDefender positively impacts my organization by filling the gap, as we do not have any other product that can scan API calls. It has helped to improve compliance requests. It also scans all the API traffic and makes sure the API traffic is secured and clean..”

Kevin-Liu

Information Security Consultant at a tech vendor with 51-200 employees

[Read full review](#) 

“The best features MetaDefender offers, in my opinion, are that it adapts the policies on the go, and that is the best feature.

“When I say it adapts policies on the go, it has the ability that if there is a new policy or the new configuration that has come up without any downtime, it just adjusts it and reiterates to all of the users and all of the devices. MetaDefender has positively impacted my organization as it has reduced time for the users.

“MetaDefender reduces time for users in their working, as it does not occupy the RAM usage of their devices plus it does not take time for the downtime or shutting down or the rebooting of the devices..”

Rajkumar Gupta

Manager, Ibms Projects Operations & Corporate Information Technology at
Yotta Infrastructure Solutions LLP

[Read full review](#) 

“The best features of MetaDefender include its ability to detect malware and vulnerabilities, which I also use at server levels, including production and testing servers, helping me identify and address vulnerabilities by applying patch updates.

“When sanitizing files based on policies, MetaDefender processes and sanitizes files to remove hidden content, including embedded objects and scripts while preserving the visible content.

“I use MetaDefender Archive Extractor, which supports over 30 archive file types, improving detection and preventing archive bombs, allowing administrators to perform archive handling once for each file type..”

DineshKumar31

Packaged Application Development Team Lead at Accenture

[Read full review](#) 

“The best features of MetaDefender include multi-scanning, multi-layered scanning of any email or attachment, the CDR feature, and the sandboxing analysis capability. The multi-scanning feature is particularly useful because a file can be checked against multiple antivirus engines instead of relying on a single detection engine. Deep CDR is one of the strongest features because instead of only detecting whether the file is malicious, it can sanitize supported files by removing potentially dangerous content and reconstructing a safe version. This is especially useful for documents and email attachments where we still need to allow the business to work with the file. The adaptive sandbox is another valuable feature for files that require deeper behavior analysis, providing another layer for identifying suspicious or malware-like content that may not be obvious through the traditional scanners that we use.

“MetaDefender has a positive impact by adding multiple layers of file scanning, email classification, and attachment investigation in a more efficient way. Instead of just relying on the verdict from our primary email or endpoint security solution, we can use MetaDefender to get additional analysis across multiple engines. This is especially helpful when dealing with suspicious or previously unseen files, zero-day attack files. Deep CDR has also been useful from a risk reduction perspective because potentially dangerous content can be removed from supported files while still allowing users to work with a usable version of the document. Overall, MetaDefender has a positive impact on analysis and detecting suspicious files, leading to greater confidence in our environment. It has also helped reduce some of the manual efforts involved in determining whether the attachment is safe or not..”

Prajwal Chougale

SOC L2 Analyst at a tech services company with 51-200 employees

[Read full review](#) 

“MetaDefender's threat detection ratio is quite high because it uses multiple anti-malware engines. Sanitization helps eliminate typical zero-day threats such as macro-based attacks and script-based attacks.

“Deep CDR feature in reconstructing files has provided significant value to customers. When they receive phishing links, dummy QR codes, or embedded actions defined on documents, Deep CDR removes all those potential threats.

“MetaDefender supports all expanded file type and archive coverage features, which means most of the 4,000-plus file types are covered. It provides a quite deep scanning process. Archive extraction gives more visibility of the files.

“The file-based vulnerability assessment feature is straightforward. When downloading a file from the internet and scanning it, information about known vulnerabilities is provided. It gives advanced information about the vulnerability.

“With MetaScan multi-scanning feature, certain web shell attacks can be detected which others cannot. Whether it's 8 anti-malware engines or 20, the detection ratio and rate are quite good..”

JaiminDalwadi

Delivery Lead at altisec

[Read full review](#) 

“MetaDefender offers multiple features. Multi-scanning technology allows you to use simultaneous scanning anti-malware scanning engines to detect the malicious content of the file. It scans files using Content Disarm and Reconstruct and if any malicious content is found, then it removes that part of the content and reconstructs the file. It also uses machine learning technologies to optimize the file scanning process and has an adaptive sandbox which detects advanced persistent threats from the files.

It features proactive data loss prevention which scans all formats while sending files outside to help maintain compliance with PCI, GDPR, file-based vulnerabilities, and software bill of materials, identifying vulnerabilities in files and software components to secure supply chains. The best thing about it is we use this on cloud-native security, thus it supports cloud applications.

The effectiveness of MetaDefender in blocking or sanitizing content based on policy is evident in multiple points, such as having a multi-scanning engine detecting threats where we use multiple antivirus engines simultaneously to scan files with accuracy and block threats. It helps enforce policies such as blocking executable files, disallowing macros in office files, or restricting certain file types, enforced consistently across the endpoint, email, and file transfers. Regarding sanitizing content, these features remove active contents such as scripts, macros, and embedded objects while preserving the legibility of the file and neutralizing zero-day exploits in hidden documents or images, making it useful.

Content Disarm and Reconstruct features remove active contents such as scripts, macros, and embedded objects while preserving the eligibility of the file, ensuring the file remains usable even if malicious contents are blocked..”

Ravi Raushan Singh

Senior Associate at a educational organization with 11-50 employees

[Read full review](#) 

Other Solutions Considered

“I have previously used other endpoint products like Fortinet's FortiEDR, but only in a virtualized environment. I could do similar use cases with that one as well..”

Paul Mhiripiri

Networks And Infrastructure Manager at a financial services firm with 11-50 employees

[Read full review](#) 

“The decision to switch to MetaDefender was mainly taken by higher management, and as a SOC analyst, I was not involved in the evaluation of other options..”

Prajwal Chougale

SOC L2 Analyst at a tech services company with 51-200 employees

[Read full review](#) 

“Previously, we were using McAfee antivirus scan servers for ICAP filters, but with increasing API call requests, MetaDefender filled that gap and provided the API call scan service, which is great..”

Kevin-Liu

Information Security Consultant at a tech vendor with 51-200 employees

[Read full review](#) 

“Before choosing MetaDefender, we did not evaluate other options. We mainly wanted to use OPSWAT for API call scans, and we could not find any other product in the market at that time..”

Kevin-Liu

[Read full review](#) 

Information Security Consultant at a tech vendor with 51-200 employees

“I did not evaluate other options; it was directly notified by higher management that we were going to use MetaDefender. They had evaluated it at their level, and I only know of some tools that were considered, namely Symantec Endpoint Protection and Trend Micro Deep Discovery..”

Ravi Raushan Singh

[Read full review](#) 

Senior Associate at a educational organization with 11-50 employees

“I have evaluated other options available in the market, such as Microsoft and McAfee, but found MetaDefender to be distinct.

“I decided to go with MetaDefender due to its architectural compatibility with the client's budget requirements, as its scanning and vulnerability detection capabilities are better than other tools..”

DineshKumar31

[Read full review](#) 

Packaged Application Development Team Lead at Accenture

ROI

Real user quotes about their ROI:

“Many threats are prevented before entering the organization with MetaDefender. It definitely saves more effort for the SOC team if threats are being eliminated at the entry point itself, allowing them to focus more on other things..”

JaiminDalwadi

Delivery Lead at altisec

[Read full review](#) 

“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 have reduced some of our manual effort and saved time, even investing additional time on zero-day attacks. In file analysis, we have sometimes saved a lot of time, while also spending a little more on suspicious files. Overall, using MetaDefender has been beneficial and can be justified as a positive investment..”

Prajwal Chougale

[Read full review](#) 

SOC L2 Analyst at a tech services company with 51-200 employees

“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

[Read full review](#) 

Network Security Engineer at EMAK For Integrated solutions

“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

[Read full review](#) 

Manager at Cyvogenix

“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 major use cases of MetaDefender in my work environment involve preventing malware updates, data breaches, and compliance violations through scanning files for malware, vulnerabilities, and sensitive data at the network perimeter..”

DineshKumar31

Packaged Application Development Team Lead at Accenture

[Read full review](#) 

“I am an integrator for MetaDefender. My usual use cases for MetaDefender involve connecting the products into the environment of the customer, including MetaDefender Core, ICAPs, endpoints, and all the related components..”

Alex Nigai

Integration Technician at danet

[Read full review](#) 

“My main use case for MetaDefender is on my devices. I have a specific example of how I use MetaDefender on my devices in that it has been installed by the administrator on my VMs which are being listed on my public cloud.

“I don't have anything specific to add about how I use MetaDefender in my setup, as it is protecting my whole VMs, so not any particular file..”

Rajkumar Gupta

[Read full review](#) 

Manager, Ibms Projects Operations & Corporate Information Technology at
Yotta Infrastructure Solutions LLP

“My main use case for MetaDefender involves the Central Management Console, core service, and ICAP service.

In my day-to-day work, I use MetaDefender to scan endpoint security, but we did not have a product to cover API traffic scans. MetaDefender OPSWAT provides that solution, and also the ICAP scans. It is a really good product. We have customers sending all the files via API calls, and they will be scanned by OPSWAT for antivirus scan and also Data Loss Prevention scan. It is a great product.

We have more than ten different vendors connected to MetaDefender for scanning, and it is working very well..”

Kevin-Liu

[Read full review](#) 

Information Security Consultant at a tech vendor with 51-200 employees

“My main use case for MetaDefender is for multi-scanning purposes, including Deep CDR, sandbox-based analysis, and protecting the organization from malware and other file-based threats delivered through email, particularly suspicious or unknown attachments. I primarily view it as an additional inspection layer for email attachments, using its multi-scanning capability to analyze files with multiple detection engines. The Deep Content Disarm and Destruction capability is also valuable because it can remove potentially malicious content from supported files and provide a safer version for the user. From a SOC's perspective, this is particularly useful for handling files that may bypass traditional signature-based security controls while email filtering is happening. It gives us additional confidence when dealing with documents such as PDFs and Office files and all other materials that we receive through email. MetaDefender prevents malicious or weaponized files from reaching users while reducing the risk associated with unknown, zero-day file-based threats..”

Prajwal Chougale

SOC L2 Analyst at a tech services company with 51-200 employees

[Read full review](#) 

“In my organization, I use MetaDefender for scanning incoming and outgoing files for any malicious content, and if any malicious content is found, then I filter it out using this tool.

While I was working with the bank, there are multiple vendors or partners who were sending and receiving files to and from the bank, and few files are coming from outside of the organization. We had a doubt that if any outsider sends files to us and if it is malicious, then it can create an issue on the server. So, we implemented MetaDefender for scanning all incoming and outgoing files and in that, in a month, we scanned over 10 million files and we found out of those, around 60 files were found malicious.

MetaDefender is a useful tool for scanning all incoming and outgoing files and keeping our applications and servers in compliance, and I found it useful because we can integrate it with multiple file transfer tools such as Globalscape EFT, GoAnywhere, or Sterling, which is the best feature as it integrates with multiple tools.

I transfer around millions of files in my organization, one million files daily, and while we implemented scanning with MetaDefender, we found out that every day we are transferring one or two malicious files, which were filtered out and relevant stakeholders were notified. They corrected it and we sent it to the security team who analyzed it, further helping us keep our systems clean..”

Ravi Raushan Singh

Senior Associate at a educational organization with 11-50 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 decision to switch to MetaDefender was mainly taken by higher management, and as a SOC analyst, I was not involved in the evaluation of other options..”

Prajwal Chougale

[Read full review](#) 

SOC L2 Analyst at a tech services company with 51-200 employees

“We saved a lot of time for scanning files. Earlier, multiple teams from each department scanned files. However, with the implementation of MetaDefender, we could scan all incoming and outgoing files at a single point, and if any files needed further attention, they could easily be found in reports which we shared through SIEM with multiple teams..”

Ravi Raushan Singh

[Read full review](#) 

Senior Associate at a educational organization with 11-50 employees

“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 initial deployment is straightforward, as there is an enroll link on the portal. Clicking that gives me options to enroll in MetaDefender Core, Endpoint, or Industrial File. I receive a QR code, and for devices like phones, scanning it enrolls them automatically. For Windows devices, it provides links to download the EML or EXE files, enabling easy Active Directory use. This straightforward enrollment process applies to Linux and macOS as well. However, for IoT devices, it is not so straightforward since it requires building the application from a downloaded file and running it, especially for Linux-based IoTs..”

Paul Mhiripiri

Networks And Infrastructure Manager at a financial services firm with 11-50 employees

[Read full review](#) 

“I participated in the initial setup and deployment of MetaDefender. The initial setup process was pretty easy. There were a few problems with the SSO configuration, but everything else was pretty straightforward. To integrate the platform and install it very fast and in a good manner, you should plan it very well and understand exactly what your environment is in the company. Whether you are going to install it on-premise or in the cloud environment as a VM or any other solution that they are suggesting. I did not see any problems except the SSO configuration. Everything else was pretty fast and convenient..”

Denis Burnaev

[Read full review](#) 

Infrastructure Security & Cyber Engineer at El Al

“I usually participate in the initial setup, including the installation of MetaDefender. Most of the time, I send requirements for the server, and the customer has to create a server that meets what I have requested. After the customer has made the prerequisites, I can work with them on installing and connecting the products into their environment.

“The initial setup usually looks like this for me: first, I need to send the prerequisites for every product, and I reference OPSWAT documentation to see what is needed, such as Visual Studio or Desknet. Then I send downloads of the products.

“I usually find the initial setup has small challenges such as connectivity issues, but these are not on OPSWAT's side. They are more related to the customer's environment..”

Alex Nigai

[Read full review](#) 

Integration Technician at danet

Customer Service and Support

“Their customer support is outstanding. Whenever we raise any support case, they provide complete structural descriptions and solutions to the problems we report, and they resolve issues on the spot. I would rate them nine out of ten..”

Prajwal Chougale

SOC L2 Analyst at a tech services company with 51-200 employees

[Read full review](#) 

“Customer support is great. I have worked with the Vietnam team quite a few times, and they are always very active, proactive, and offer remote sessions quite a few times. It is a great service..”

Kevin-Liu

Information Security Consultant at a tech vendor with 51-200 employees

[Read full review](#) 

“I have not contacted technical support, though I thought I might need assistance fine-tuning my policy. When MetaDefender flagged some Windows DLL files as infections, I looked up information online and needed to whitelist them if they run directly from the Windows folder. If I could not resolve that, I would reach out for support, but I have not raised any tickets with MetaDefender yet..”

Paul Mhiripiri

[Read full review](#) 

Networks And Infrastructure Manager at a financial services firm with 11-50 employees

“I do not often communicate with the technical support of MetaDefender, only with the integration team. I am happy with my interaction and communication with MetaDefender's team. The communication was great and understanding. It was easy because I was familiar with OPSWAT Core, not so much with MetaDefender, but with OPSWAT Core I was familiar, and the policy and everything else that you configure on OPSWAT Core. The communication was great..”

Denis Burnaev

[Read full review](#) 

Infrastructure Securiy & Cyber Engineer at El Al

“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

[Read full review](#) 

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

“When I need help, I reach out first by trying to find information in the documentation. If I cannot find that, I go to the Ozi AI. If I see that the AI cannot help me, then I ask for an agent.

“When it comes to my communication with agents, I find they are responsive and professional. A lot of the time, they are busy, so they cannot participate in calls or Teams meetings. However, if we schedule a meeting, they will attend, especially if it is very important..”

Alex Nigai

[Read full review](#) 

Integration Technician at danet

Other Advice

“If you are looking for a solution that enhances your email security or your EDR product, and if you are considering more security solutions that can protect both combinedly, I would recommend MetaDefender as one of the best tools. Its features include multi-scanning, Deep CDR, sandboxing, and file investigation, which are essential for effective detection while minimizing false positives and scanning times. Integration with the existing environment is also important; if you are using Microsoft 365, ensure that flow connectors and policies are planned and tested before moving into production. I would also check for potential conflicts or mail loops if another third-party email security solution is already deployed. Another recommendation is to spend time on policy tuning and user group segmentation. MetaDefender allows policies to be prioritized and applied to specific audiences, making administration much easier as the environment grows. I would recommend this approach as well. My overall rating for MetaDefender is eight out of ten..”

Prajwal Chougale

SOC L2 Analyst at a tech services company with 51-200 employees

[Read full review](#) 

“My advice to others looking into using MetaDefender is that it is a great product. We are only using the on-premise product because of company policy, as we are not allowed to upload our customer data into the public cloud. I think the hybrid cloud and private cloud product would be beneficial. That is the trend, so using hybrid cloud mode is a beneficial option for all other companies. We are currently still using the on-premise product.

We are not using the enhanced reporting and audit visibility features at this time.

The file-based vulnerability assessment feature is great because it can scan using seven different antivirus scan engines, but with AI attacks now, signature-based detection is not sufficient, which is a problem for all antivirus product vendors.

I give MetaDefender an overall rating of ten out of ten..”

Kevin-Liu

Information Security Consultant at a tech vendor with 51-200 employees

[Read full review](#) 

“MetaDefender is leading with respect to competitors as an all-in-one platform because no other tool has all the platform built-in.

“For example, MetaDefender cannot identify the source itself, but if a file is scanned, the complete detail of the scanning can be seen.

“If someone modifies a policy, adaptive sandbox analysis takes a little bit of time, but it gives accuracy up to 99%.

“Continuous improvement that OPSWAT is doing with enhancements made to policy orchestration and to engine parallelization demonstrates that OPSWAT is adapting.

“I rate this solution a 10..”

JaiminDalwadi

Delivery Lead at altisec

[Read full review](#) 

“If anyone is using file transfers or wants to monitor their files and emails to scan attached files, MetaDefender is a useful tool where you can integrate your file transfer tool with MetaDefender, which is a plug-and-play solution supporting both cloud and on-prem involvement, making it very useful.

I deducted those two points because there were a number of times where I was getting false positive results and it took time to scan files if the file size was greater than 1 GB.

In multi-scanning engine, the best part is that it scans all the components of the file, removes the malicious content, and reconstructs the file, which is excellent.

For sandbox analysis, there was another team working with it, so I was not using it actively.

I was using audit visibility features, which helped me keep our systems error-free and bug-free. Whenever we found any file with malicious content, we reported it to the security team, they analyzed it further, and we informed relevant stakeholders who took further actions. I gave this review a rating of 8 out of 10..”

Ravi Raushan Singh

Senior Associate at a educational organization with 11-50 employees

[Read full review](#) 

“My impression of the detection rates provided by MetaScan Multi-scanning is that it is good and pretty accurate. I would assess the effectiveness of Deep CDR in reconstructing files safely and without signatures as they are pretty much effective, and it is really useful for the administrator.

“My thoughts on the file-based vulnerability assessment feature in identifying vulnerabilities before deployment are that it is good, and it is a very good feature. I use adaptive sandbox analysis, and its impact on analyzing suspicious files is very

great because it detects pretty much early.

“I am using the enhanced reporting and audit visibility features, and they have helped meet our audit requirements as it has given us a great requirement study and plus it has also helped in ISO audit requirement as well. I would assess the effectiveness of the solution in blocking or sanitizing content based on policy as good and pretty much effective.

“My advice to others looking into using MetaDefender is that if you are looking ahead at a solution which can be implemented quickly and at a lesser cost, go ahead with it. I would rate this product an eight overall..”

Rajkumar Gupta

Manager, Ibms Projects Operations & Corporate Information Technology at
Yotta Infrastructure Solutions LLP

[Read full review](#) 

“The detection rates from MetaScan multi-scanning are managed mainly by other teams in alignment with our organization policy, where they can achieve detection rates of 81–87% with four engines or 95% with sixteen engines, and the comparison with Microsoft Defender often yields similar results.

“I do not have an opinion on the effectiveness of Deep CDR in file reconstruction.

“We have a process in place for identifying vulnerabilities before deployment where team members raise tickets on the [ServiceNow](#) portal for the respective teams to address.

“I do not use Adaptive Sandbox analysis, as that is managed by another team.

“I do not notice improvements in workflow automation as recent enhancements are managed by other teams; I am focused on using the tool to identify vulnerabilities.

“I do not have an assessment of how multi-scanning and content disarm and reconstruction affect our data security operations.

“I recommend implementing MetaDefender for its impressive features that maintain the health of the system. My overall review rating for MetaDefender is nine out of ten..”

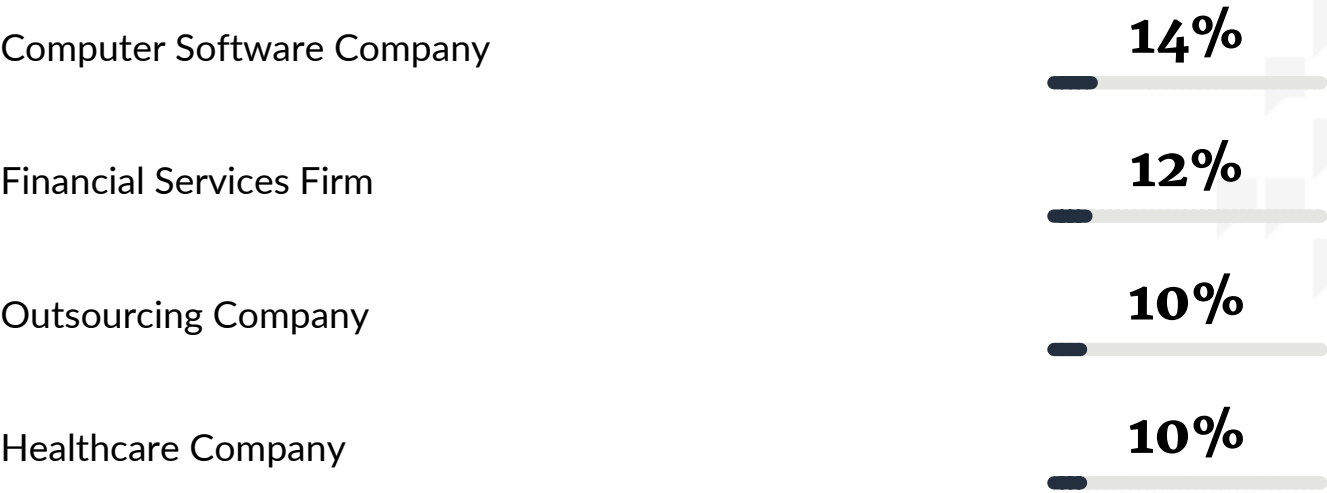
DineshKumar31

Packaged Application Development Team Lead at Accenture

[Read full review](#) 

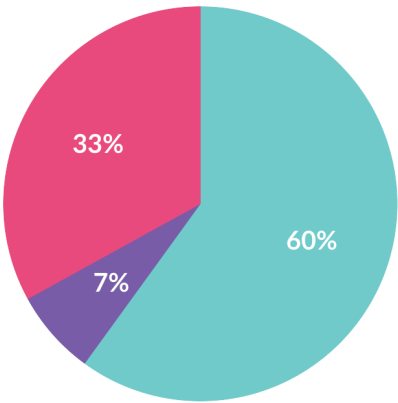
Top Industries

by visitors reading reviews

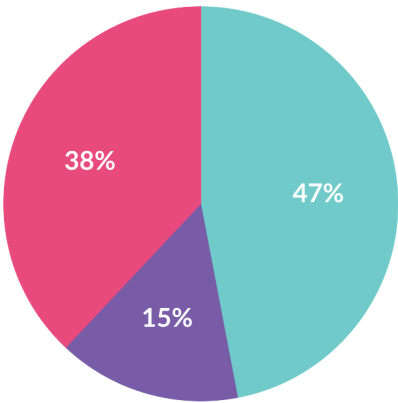


Company Size

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 cloud, AI, and business software. We created PeerSpot to provide a trusted platform to share information about software, applications, and services. Since 2012, over 22 million people have used PeerSpot to choose the right software for their business.

PeerSpot helps tech professionals by providing:

- A list of products recommended by real users
- In-depth reviews, including pros and cons
- Specific information to help you choose the best vendor for your needs

Use PeerSpot to:

- Read and post reviews of products
- Access over 30,000 buyer's guides and comparison reports
- Request or share information about functionality, quality, and pricing

Join PeerSpot to connect with peers to help you:

- Get immediate answers to questions
- Validate vendor claims
- Exchange tips for getting the best deals with vendor

Visit PeerSpot: www.peerspot.com

PeerSpot

244 5th Avenue, Suite R-230 • New York, NY 10001

reports@peerspot.com

+1 646.328.1944