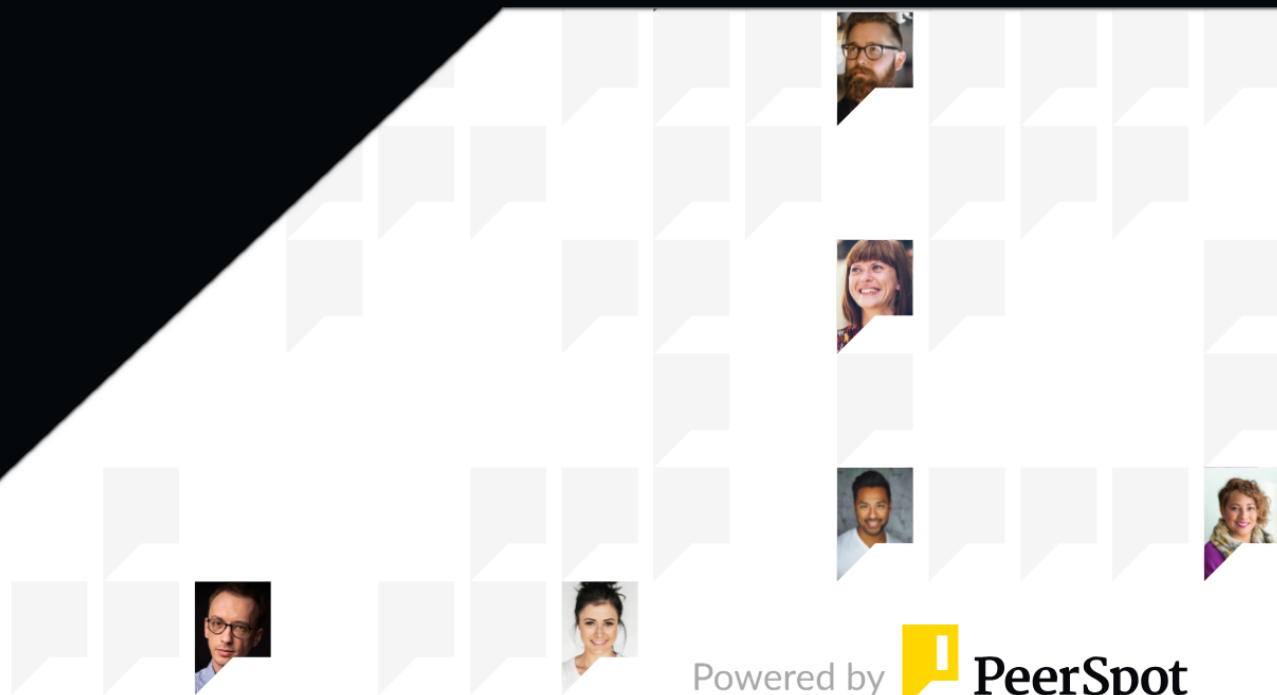


aws marketplace

MetaDefender

Reviews, tips, and advice from real users



Powered by  **PeerSpot**

Contents

Product Recap..... 3 - 4

Valuable Features..... 5 - 13

Other Solutions Considered..... 14 - 15

ROI..... 16 - 18

Use Case..... 19 - 23

Setup..... 24 - 26

Customer Service and Support..... 27 - 29

Other Advice..... 30 - 34

Trends..... 35 - 36

About PeerSpot..... 37 - 38

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.”



Validated 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 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 checks all the software and its latest version, and whether the local software that is installed is aligned with the organization policy that is set by the organization security administrator. MetaDefender passes all this information and checks against those policies that are being set and determines whether the installed software is aligned with the organization policy or not. For example, if any deprecated software or any software that has any kind of malware is in the machine, then it immediately highlights and stops accessing those protected resources.

“MetaDefender is always on at startup; it must be enabled during startup of the operating system, and when accessing any protected resource, after authorization and authentication, it immediately checks whether the resource being accessed is allowed for access, and it scans all the software. Whether it is a browser version such as Chrome browser, or if it is having a deprecated or older version, or any operating system software such as WinRAR or Notepad++, any software that is deprecated or has an older version, it will immediately flag that as an error and will not allow access to the protected resources.

“This is quite helpful in terms of securing resources; it immediately brings those vulnerabilities or incompatibilities in the system to attention. It also provides the feature to check the status of the operating system or machine status immediately. There is an icon at the taskbar; clicking and rechecking the status of MetaDefender Endpoint shows the current status. If all are acceptable, then it will confirm that all is well, and access to the protected resources can proceed. If there is any issue, it will flag that on the screen when rechecking the status.

“MetaDefender highlights all the vulnerabilities the moment of accessing the protected resources, so it scans all the files in the system and brings those issues when clicking the recheck button.

“It does the auditing of the local machine and maintains awareness of what is occurring on the machine, specifically from the security perspective. If there is any vulnerability or any kind of malware being deployed in the machine, it immediately stops access to those protected resources..”

“In my experience, MetaDefender offers a Deep CDR, and other major strengths include multi-scanning, Tri-tech AI, Adaptive Sandbox, Proactive DLP, and file vulnerability assessment.

“Out of those features, I find myself relying on Deep CDR the most because it is one of MetaDefender's key differentiators; it does not depend only on detecting known malware but sanitizes and reconstructs files to prevent potentially malicious content, including zero-day threats, from reaching the environment.

“Regarding MetaDefender's AI features, I think it handles data responsibly and keeps things secure by providing protection in multiple layers through malware scanning, threat detection, and content sanitization, which helps organizations manage security risks while maintaining a good balance between security, control, and compliance.

“I find MetaDefender's AI capabilities to be reliable and useful as an additional layer of threat detection, with results that have been generally consistent and provide useful insights when analyzing files, though I have not used the AI capabilities long enough to independently measure accuracy.

“My impression of the detection rates from MetaDefender's Metascan Multi-scanning has been positive; using multiple scanning engines provides broader coverage and greater confidence that potential threats will not be missed, and while I have not independently measured the detection rate, the results I have seen are consistent and useful for identifying potential malicious files.

“I assess Deep CDR as highly effective in reconstructing files safely and without signatures because it focuses on safely reconstructing files rather than relying only on traditional malware signatures, which is particularly valuable for handling unknown or potentially zero-day threats while keeping reconstructed files usable.

“I think the file-based vulnerability assessment feature is valuable because it helps identify potential vulnerabilities before files or applications are deployed, providing an additional preventive security layer that helps organizations address risk earlier rather than discovering them post-deployment.

“We are using the reporting and audit visibility features to gain better visibility

into scanning activities and results, which help provide a clearer record of what has been scanned and the outcomes, aiding in tracking and audit purposes from an operational perspective..”

Sriparna Banerjee

Senior Project Engineer at a tech vendor with 10,001+ 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

“Previously, the authentication and authorization method was using Azure Active Directory, or Azure Entra ID, and now MetaDefender is also used along with Azure AD..”

Pradeep Dubey

[Read full review](#) 

Solution Architect at Tata Consultancy Services

“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:

“MetaDefender Endpoint has provided benefit from its use. The company's resources are fully protected and secured; no unauthorized access can reach the protected resources. All resources are now secured, and MetaDefender Endpoint can be trusted in this area..”

Pradeep Dubey

Solution Architect at Tata Consultancy Services

[Read full review](#) 

“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

SOC L2 Analyst at a tech services company with 51-200 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](#) 

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](#) 

“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

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

[Read full review](#) 

“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

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

[Read full review](#) 

“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](#) 

“My main use case for MetaDefender is for security purposes, as we are a cybersecurity team, and currently we are using it for purposes such as antivirus scanning and other security measures.

“In my day-to-day work, we are working with a company called Opswat, and we have devices, so to keep everything clean and clear, we are using MetaDefender as an antivirus firewall. We are inserting this MetaDefender chip for scanning purposes and using it as a firewall as well, but I do not have much knowledge about it because I am in a non-technical role right now.

“In terms of using MetaDefender, we are utilizing it for threat detection, multi-scanning, and enterprise security..”

Sriparna Banerjee

Senior Project Engineer at a tech vendor with 10,001+ employees

[Read full review](#) 

“Before accessing the company's protected resources, it is being scanned through MetaDefender Endpoint, which scans the local operating system and machine before the request actually hits the company's protected resources.

“MetaDefender Endpoint has been installed in the Windows operating system machine, and before accessing any protected resource of the company, MetaDefender scans the request and the resources, and it even scans the local machine. If there is any vulnerability or any kind of malware, then it immediately blocks the resource and does not allow access to the protected resource for the company. In this case, it is the company's protected resource, so access is not allowed. It checks the software and checks the various software that is installed in the machine, and if all are acceptable, then only MetaDefender is allowed to access the protected resources.

“For companies that are widely distributed and have resources with company employees widely located across the world, it provides a centralized, secure platform before accessing any protected resource. This is a mandatory software that everyone should install in their machine and ensure that it passes all the quality checks, making it a strong platform in terms of security and securing protected resources..”

Pradeep Dubey

Solution Architect at Tata Consultancy Services

[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

[Read full review](#) 

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

“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

[Read full review](#) 

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

“Customer service has not been contacted yet because it is a quite stable environment and a stable platform. MetaDefender highlights all the issues and even guides how to resolve vulnerabilities, for example, by installing upgraded software or conducting a full scan. It is quite comprehensive in explaining the issues that are currently encountered..”

Pradeep Dubey

[Read full review](#) 

Solution Architect at Tata Consultancy Services

“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

“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

Integration Technician at danet

[Read full review](#) 

Other Advice

“From the security perspective, I would rate it an eight. MetaDefender is on-premises and managed by the company's platform. For any company where resources are widely located across the globe, MetaDefender Endpoint should be considered as one of the security platforms that ensure all protected resources are very much secure..”

Pradeep Dubey

Solution Architect at Tata Consultancy Services

[Read full review](#) 

“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 offers strong security capabilities and multiple layers of threat detection, but since I am still relatively new to this platform, I would explore more of its features before giving it a higher rating. Even though MetaDefender provides a strong, multilayered security and is quite useful and comprehensive, the user experience on onboarding and the clarity of scan results could be simpler, especially for new users.

“My advice to organizations looking into using MetaDefender is to seek an additional layer of security around file and content handling, as it is a great choice with multi-engine scanning, CDR, and vulnerability assessment capabilities providing good overall coverage. It is important to clearly understand your organization's security requirements and take time to explore the different features and integrations to get the most value from the platform.

“I would rate MetaDefender as an eight out of ten..”

Sriparna Banerjee

Senior Project Engineer at a tech vendor with 10,001+ 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](#) 

“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..”

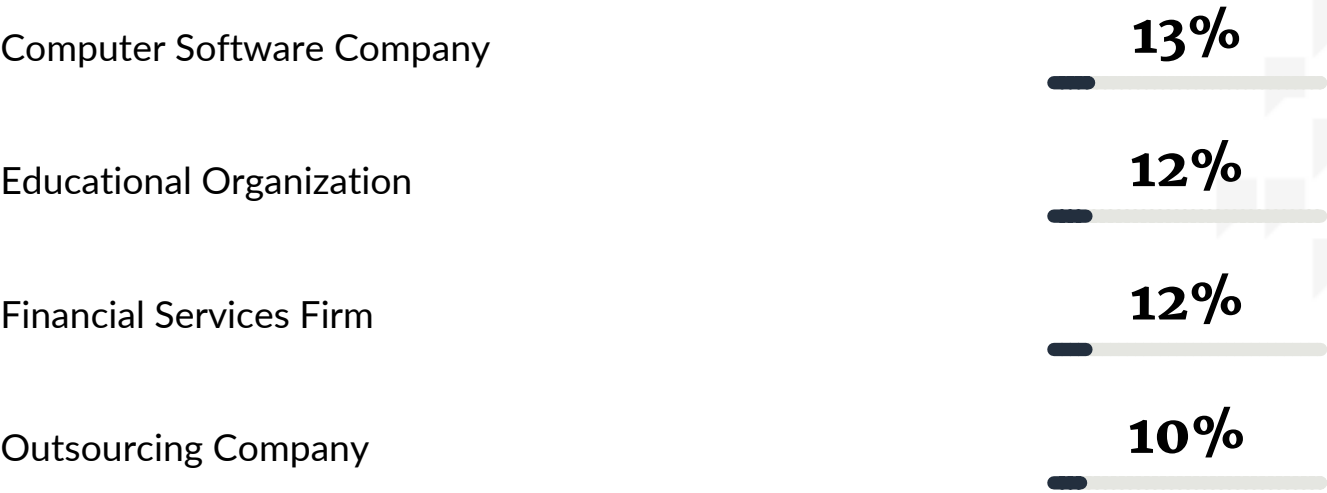
Rajkumar Gupta

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

[Read full review](#) 

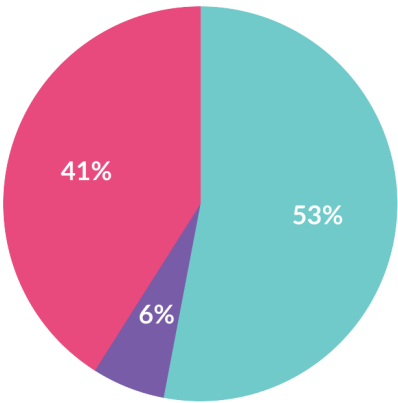
Top Industries

by visitors reading reviews

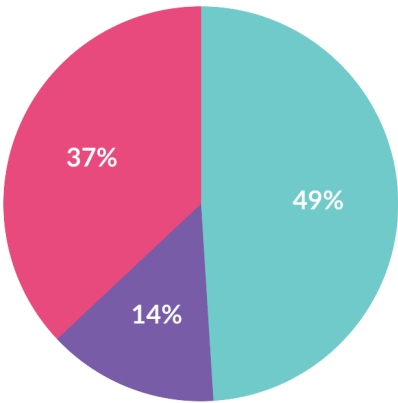


Company Size

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 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