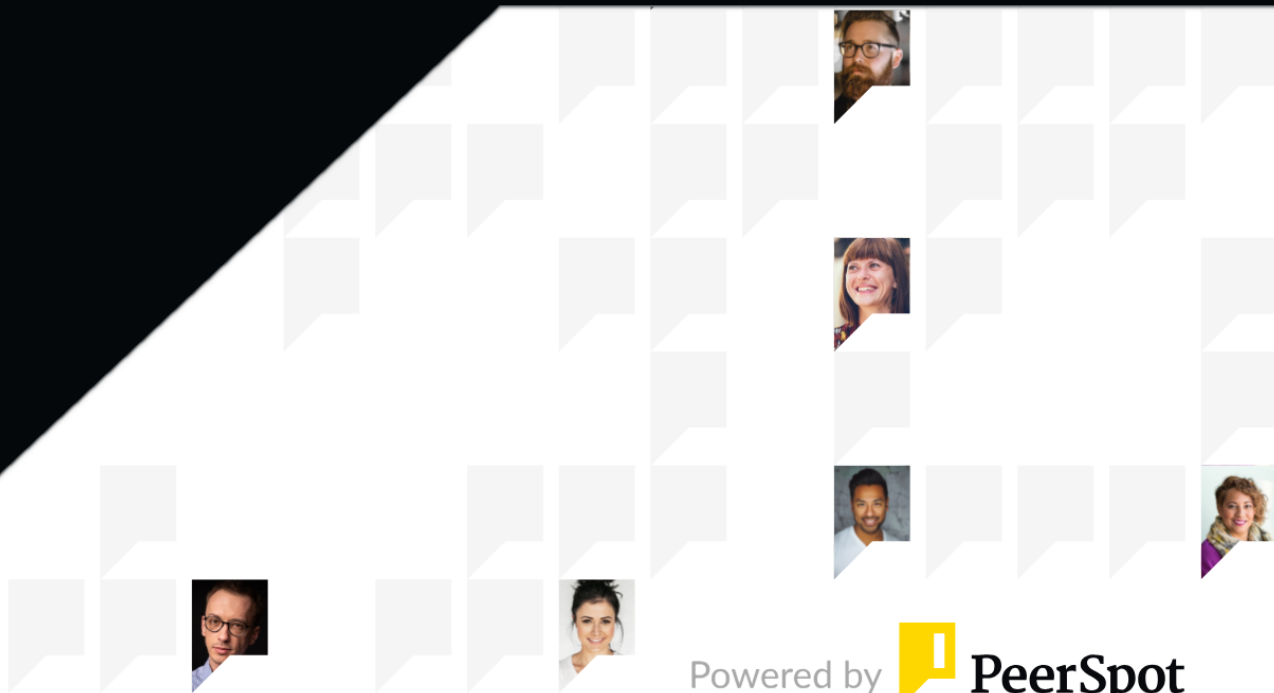


aws marketplace

MetaDefender

Reviews, tips, and advice from real users



Powered by  **PeerSpot**

Contents

Product Recap..... 3 - 4

Valuable Features..... 5 - 14

Other Solutions Considered..... 15 - 16

ROI..... 17 - 19

Use Case..... 20 - 25

Setup..... 26 - 28

Customer Service and Support..... 29 - 31

Other Advice..... 32 - 35

Trends..... 36 - 37

About PeerSpot..... 38 - 39

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 Infra Architect 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:

“In my experience, the best feature that MetaDefender offers is its perfect documentation, which is critical for API integrations to ensure files are not corrupted or infected with viruses.

I would add that for the dashboard, while I have used it, I am more fascinated about the API. It is good that we can manage users from one console, and I can see the history of uploads and whether the files are corrupted or not.

I think the detection rates provided by MetaDefender through multi-scanning are good, as it stops almost all of the virus files I have uploaded.

MetaDefender effectively blocks the harmful content based on our policies, as this is working perfectly fine for me, though I cannot share specific policies..”

Sandeep Parmar

Back End Software Engineer

[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](#) 

“The best features MetaDefender offers in my experience include how easily it installs and the great GUI that I find excellent, even though I feel quite confused with the new version. I appreciate how everything connects smoothly, which allows my workflow to cover more directions in my company.

“I find the new GUI confusing only because I am used to the previous one. While it is common to need time to adjust to a refreshed GUI, overall, the GUI is still one of the best I have ever seen. Connecting different modules is easy to do, just as installing on your Linux or Windows system and configuring it to work out of the box is straightforward.

“I have a great impression of the detection rates provided by MetaScan multi-scanning. It is one of the best I have ever seen.

“I assess the effectiveness of Deep CDR in reconstructing files safely and without signatures as a ten out of ten, as I really appreciate how it is done.

“The file-based vulnerability assessment feature is useful for identifying potential security risks before deployment, as it helps to detect vulnerabilities at an early stage and reduces the risk of introducing vulnerable components into production environments.

“We use the adaptive sandbox analysis, and I appreciate it because it operates on a separate server, MetaDefender IFR. I appreciate the GUI, the design, and the overall reports it generates.

“We are using the enhanced reporting and audit visibility features because the reports are very colorful and everything we need is beautifully presented.

“I assess the effectiveness of the solution in blocking or sanitizing content based on policy as a ten out of ten..”

M Kopeichikov

Network Security Engineer at a tech services company with 51-200 employees

[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..”

“The best feature MetaDefender offers is Content Disarm and Reconstruction because if there is malware in a particular file and the agent is sitting on it with Content Disarm and Reconstruction enabled, it is going to remove the malware and give you the exact file you need without you even being aware, which is a very good technology.

“One of my experiences with Content Disarm and Reconstruction is that I intentionally wrapped a payload into a file and sent it to a particular device on the network to see if this really works. Upon the user clicking it, it was supposed to ransom the user's computer, but it was able to tell the user that this is a malicious file and it would undergo Content Disarm and Reconstruction. Upon clicking, it removed the payload and gave the user the real file beneath the wrapped malware.

“Regarding my main use case and how I use MetaDefender, the use of DLP is very important because I work in a setting where you do not want users to exfiltrate your data. Some ports have been shut down, such as USB, and we do not allow external USB devices. DLP helps us to make sure that the USB port will be disabled, and you can also shut down the device if it is stolen. You can run malware detection periodically, and you can configure a lot of policies, which I was able to do using MetaDefender on those devices.

“Regarding MetaDefender's AI capabilities, I think the governance and security are good. It is compliant and gives you an overall score of your device to see if it is compliant.

“MetaDefender has been dependable for me because if I come into contact with a roadblock, I can ask the AI, and it really helps me twenty-four hours a day, seven days a week.

“My impression of the detection rates provided by MetaScan multiscanning is that they are very reliable and can be trusted. While using it, I switched off my Windows Security to see if it would detect threats, and it did, providing recommendations that help you manage your security effectively.

“I use adaptive sandbox analysis, which places the file into a sandbox to see its behavior, and it gives me the metric for it. Regarding file-based vulnerability

assessment before deployment, it performed a vulnerability scan and provided patches without me having to look for them, and all patches were easily applied from the console screen..”

Seguntaiwo Tao

Cybersecurity Professional at a tech vendor with 1-10 employees

[Read full review](#) 

“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

“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 used different solutions such as Qualys and Nessus, and we are currently using ManageEngine to see the features of these products and make a decision. Not that either solution is bad, but we need to choose what is best by trying each of them..”

Seguntaiwo Tao

Cybersecurity Professional at a tech vendor with 1-10 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, I cannot really remember evaluating other options besides FortiSandbox and MetaDefender Core, but we ultimately chose MetaDefender Core because it was better..”

M Kopeichikov

Network Security Engineer at a tech services company with 51-200 employees

[Read full review](#) 

“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

Solution Architect at Tata Consultancy Services

[Read full review](#) 

“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

Packaged Application Development Team Lead at Accenture

[Read full review](#) 

ROI

Real user quotes about their ROI:

“I have not seen a return on investment regarding time or money, but the implementation of MetaDefender provides an essential security layer that blocks potential threats..”

Sandeep Parmar

Back End Software Engineer

[Read full review](#) 

“I cannot assess the return on investment with MetaDefender since we never invested in it. We only used the trial, and I can answer that once we make a decision on whether to proceed with it..”

Seguntaiwo Tao

Cybersecurity Professional at a tech vendor with 1-10 employees

[Read full review](#) 

“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](#) 

“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](#) 

Use Case

“The main use case for MetaDefender in the project with B***** is to ensure that files are scanned before sending them to the server, where I created a Java-based service that checks for viruses.

In the project with B*****, my main use case for MetaDefender is to scan files that use Excel uploads and basic file uploads to prevent any virus infections, so I send the file bytes to MetaDefender APIs and check for viruses.

I do not know much about Deep CDR, as my integration is mostly for scanning viruses, and we just block files that are corrupted or harmful without reconstructing them..”

Sandeep Parmar

Back End Software Engineer

[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](#) 

“My main use case for MetaDefender is to scan files from chats on a day-to-day basis, because sometimes most of the people are sending something possibly malicious via web chats, and I need to be sure that everything that comes in and comes out of that chat is legitimate and won't affect our company's computer servers.

“MetaDefender fits into my workflow for scanning files automatically. We have two MetaDefender Cores working together, and the scanning is working automatically, fast, and smoothly, while we can manually take some files from the quarantine if needed. Everything is automated with the API, so that is how we actually use it.

“During my studies, I don't really trust files from the outside, even from my professors or the internet, so I constantly scan them in MetaDefender Core and I appreciate the results. I appreciate how fast it works, and it is easy to manage, implement, and work with..”

M Kopeichikov

Network Security Engineer at a tech services company with 51-200 employees

[Read full review](#) 

“My main use case for MetaDefender involves managing endpoints and malware detection and vulnerability assessment. It is an encompassing platform that performs vulnerability assessment, endpoint protection, and malware detection.

“We were tasked to protect some endpoints, and they wanted everything to be reported to a particular dashboard, so we had to deploy the agent on each device. The deployment was very seamless, and as an admin, I could do a whole lot of things, such as disable ports, perform DLP, and use many features including Content Disarm and Reconstruction, which is very effective. We also used it on mobile devices.

“The main use case was simply protecting the endpoint and being able to do a whole lot of things remotely on those endpoints because the agent is sitting on them. It is very good for remote working, and you can be assured that your devices are protected with MetaDefender..”

Seguntaiwo Tao

Cybersecurity Professional at a tech vendor with 1-10 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

“I think my use case with MetaDefender fits into my workflow well, as it is quite easy to integrate, thanks to the thorough documentation, and we took about two or three days to integrate all of MetaDefender's APIs..”

Sandeep Parmar

[Read full review](#) 

Back End Software Engineer

“Nothing much is needed for improvements since it was linked with Active Directory, allowing all our computers online to receive the agents. We also used startup scripts to automatically start the deployment when all devices come up, so the deployment was great..”

Seguntaiwo Tao

[Read full review](#) 

Cybersecurity Professional at a tech vendor with 1-10 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 Infra Architect at a educational organization with 11-50 employees

“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

[Read full review](#) 

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

“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](#) 

“Customer support is very responsive, reaching out to me back in less than ten minutes during their work hours. There is also an AI chatbot that can provide solutions or escalate to the support team if needed. I give their customer support a perfect score of ten out of ten..”

Seguntaiwo Tao

Cybersecurity Professional at a tech vendor with 1-10 employees

[Read full review](#) 

“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

Solution Architect at Tata Consultancy Services

[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

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

[Read full review](#) 

“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](#) 

“I would rate MetaDefender around seven to eight because I have used their file scan feature, though I have not fully explored all their capabilities. I would give it a seven or eight because I have not used all the functionalities provided, and I deduct a point for the async API documentation which could be better.

Regarding MetaDefender's AI capabilities, I believe they manage governance and security policies quite well, especially since B***** is a large and reputable firm.

MetaDefender is deployed on-premises in the organization, and there is also a trial version available on the cloud, but we are currently only using on-premises.

My advice to others looking into using MetaDefender is to read the documentation first before implementing anything. I would rate MetaDefender an eight out of ten overall..”

Sandeep Parmar

Back End Software Engineer

[Read full review](#) 

“I have not used MetaDefender's AI capabilities at all because this is a new feature, and both our customers and I have not utilized AI in MetaDefender.

“I think the AI capabilities and accuracy of MetaDefender should be at the top based on my expectations, as the product overall is excellent.

“My advice for others looking into using MetaDefender is to install it on either a Linux or Windows system, conduct your tests, explore, and you will see that MetaDefender Core is an excellent product.

“I rate MetaDefender a ten out of ten..”

M Kopeichikov

Network Security Engineer at a tech services company with 51-200 employees

[Read full review](#) 

“I rate MetaDefender a nine out of ten. I chose nine out of ten because it loses that one point due to the advanced features that are probably not there and also the pricing. We used the trial method first to test the product, and for the job I needed it to cover for the SMEs, it was able to cover all the endpoints and do the job well.

“Honestly, I have not reviewed the enhanced reporting and audit visibility features, nor have I tried automating it, but it is something I am planning to do to ease my job as an administrator.

“My advice for others looking into using MetaDefender is that it is a great product with a lot of features your organization would need. The policies are easy to control, and navigation is not hard at all. Additionally, it does not take much CPU. My overall rating for MetaDefender is nine out of ten..”

Seguntaiwo Tao

Cybersecurity Professional at a tech vendor with 1-10 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..”

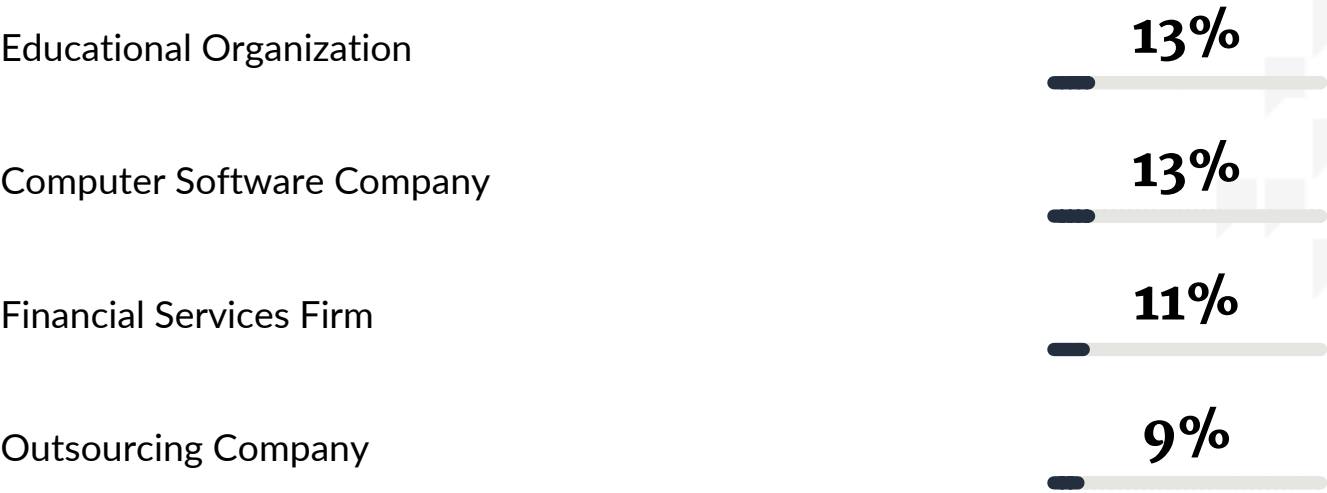
JaiminDalwadi

Delivery Lead at altisec

[Read full review](#) 

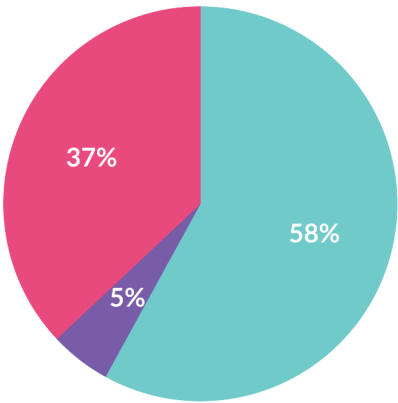
Top Industries

by visitors reading reviews

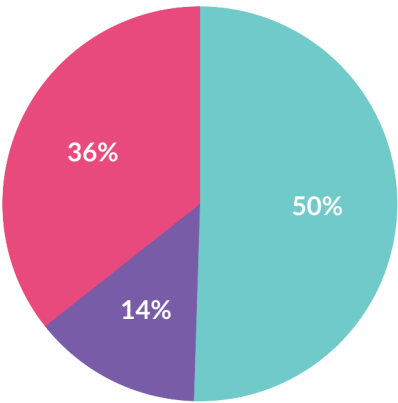


Company Size

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