aws marketplace

Antivirus for Amazon S3

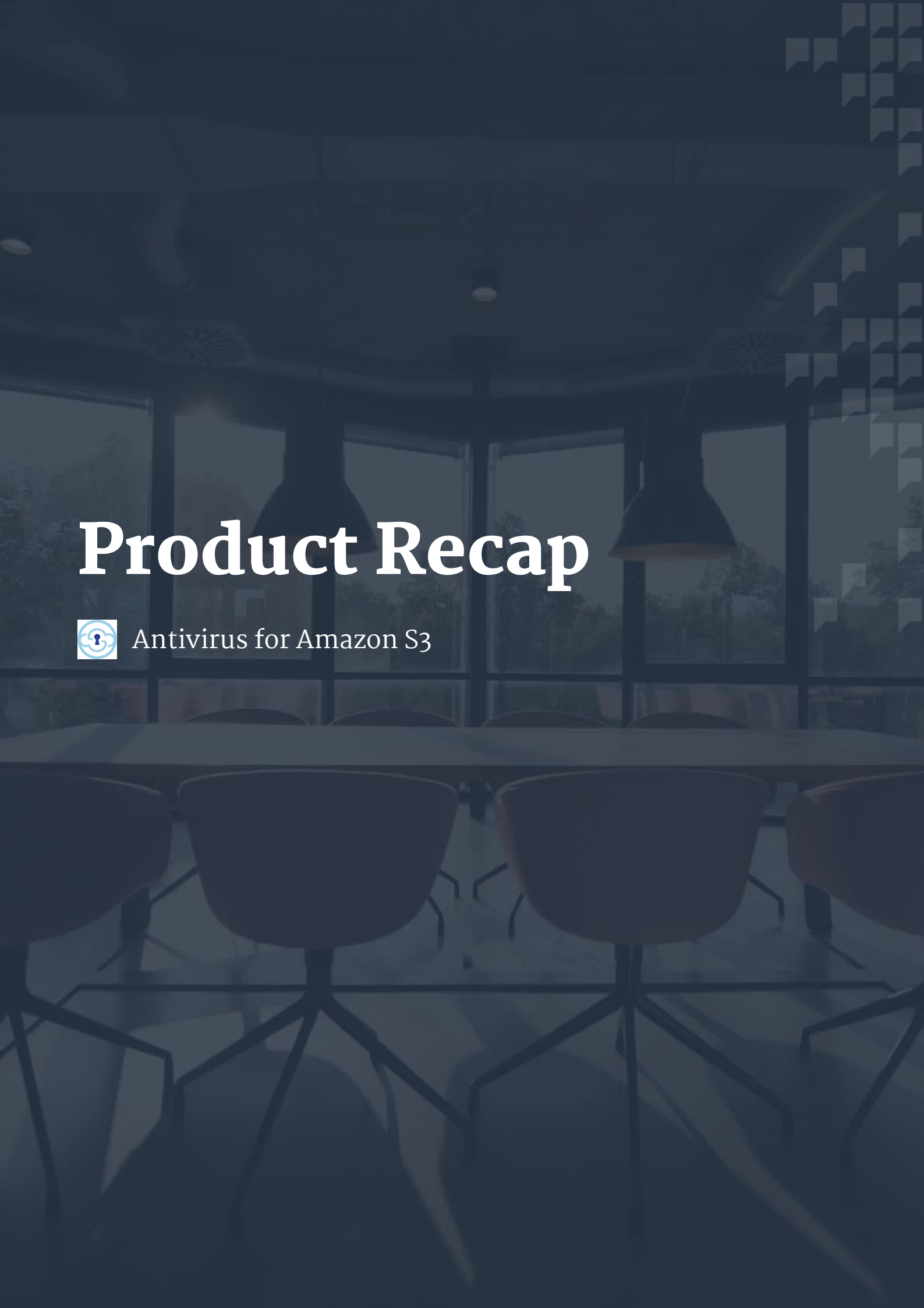
Reviews, tips, and advice from real users






Powered by PeerSpot

Contents



Product Recap

Antivirus for Amazon S3

Antivirus for Amazon S3 Recap

Antivirus for Amazon S3 is an automated security solution that discovers and scans data in Amazon WorkDocs as well as Amazon S3 buckets for threats using multiple virus detection engines.

Built on the cloud for the cloud, it enables customers to identify and remediate problem files without the need to purchase an expensive data security platform or deal with the hassles of configuring their own malware solutions.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

"Antivirus for Amazon S3 has positively impacted my organization by giving us the confidence that we can really expose our S3 buckets to the external world without having to worry about security, and from a developer standpoint, we know that at any point in time globally if S3 buckets are created, we have templates that will automatically enforce the antivirus policies there, improving our overall security posture rather than compromising it because we do have a large footprint on S3."

Kalpesh Potghante

Senior Manager at Deloitte

"Antivirus scanning has a clear positive impact on security, automation, and developer velocity in my organization."

Janindra Janekumaradi

configuration and management deployment at a tech vendor with 10,001+ employees

"In my experience, the best feature Antivirus for Amazon S3 offers is increased security."

Verified user

Cloud Ops Lead at a tech vendor with 10,001+ employees

"Integrating Amazon S3 antivirus scanning with our security monitoring systems has significantly streamlined my team's workflow and improved our response efficiency."

Vibin Thomas

Team Lead, Technical Content Security at Valuepoint Systems

"Antivirus for Amazon S3 offers some of the best features including deployment using Terraform, the ability to scan new and existing objects, very quick setup time, multiple engine support such as Sophos, CIS Premium, and CIS Secure, and extensive vendor support through many marketplaces."

AmitSharma3

DevOps Engineer at a tech vendor with 1,001-5,000 employees

"Antivirus for Amazon S3 is a great tool that is reliable and easy to integrate, adding an essential security layer for S3-based workflows which may be subject to malicious attacks and protecting the overall infrastructure while also reducing the burden of checking those files on your own."

Karan Saini

Dev Ops Engineer at a construction company with 11-50 employees

"Since using Antivirus for Amazon S3, I have seen that it is a very key feature for me as it improves compliance and also reduces risk."

Abdulsalam Abdulsalam

Security Engineer at SeaLife

What users had to say about valuable features:

"Antivirus for Amazon S3 is a great tool that is reliable and easy to integrate. It adds an essential security layer for S3-based workflows which may be subject to malicious attacks and protects the overall infrastructure while also reducing the burden of checking those files on your own. I recommend it to any organization that handles external file uploads or sensitive data in Amazon S3.

"I would rate Antivirus for Amazon S3 quite well. It is reliable and easy to integrate, adding a security layer for S3-based workloads for some of our applications. Overall, it is a good solution.."

Karan Saini

Dev Ops Engineer at a construction company with 11-50 employees

Read full review

"Antivirus for Amazon S3 offers some of the best features including deployment using Terraform, the ability to scan new and existing objects, very quick setup time, multiple engine support such as Sophos, CIS Premium, and CIS Secure, and extensive vendor support through many marketplaces.

These features benefit my workflow because whenever a Lambda is being deployed, it can be triggered at any time. While GitHub and our SCM are building it, during the time when it is being posted to S3 or being downloaded into execution, it is scanned very quickly before Lambda pulls it up, unzips it, and executes it.

Antivirus for Amazon S3 has positively impacted my organization because it has improved our bank database customer experience for our bank customers.."

AmitSharma3
DevOps Engineer at a tech vendor with 1,001-5,000 employees

Read full review

"The best features Antivirus for Amazon S3 offers include event-driven execution, automated object targeting, immediate remediation, in-tenant processing, data sovereignty, and scale and archiving support.

"Out of those features, automated object targeting stands out as the most valuable in my day-to-day work because it allows me to automatically apply a metadata tag to S3 objects as a post-scan, for instance, identifying them as infected or clean.

"I would add that you rely on humans for protection in your operation, just as you do with the automated object target. An infected tag will instantly trigger an automated workflow and bridge on AWS Lambda to immediately delete the file or move it to a completely isolated area, such as quarantine. If the file is not being deleted immediately, it is put in quarantine.."

Abdulsalam Abdulsalam
Security Engineer at SeaLife

Read full review

“Integrating Amazon S3 antivirus scanning with our security monitoring systems has significantly streamlined my team's workflow and improved our response efficiency. Earlier, live file validation and threat checks involved more manual effort and detailed analysis. After integration, the entire process became automated.

“Whenever a file is uploaded to S3, it is scanned in real-time and the results are directly sent to our SIM security monitoring tools. This has reduced our mean time to detect and mean time to respond by around 45% to 55%, as the results are generated instantly and my team can take actions without delay.

“For example, if a malicious file is detected, it is automatically quarantined and a high-priority alert is triggered, allowing us to investigate immediately. Additionally, the automation has reduced manual workload by nearly 35%, as my team no longer needs to perform repetitive file checks or validation. The solution has also improved visibility across our environment, enabling us to detect threats more effectively and respond proactively. Overall, the integration has made our security operations more efficient, faster, and more reliable..”

Vibin Thomas
Team Lead, Technical Content Security at Valuepoint Systems

Read full review

"In my experience, the best feature Antivirus for Amazon S3 offers is increased security. Because you set and forget it, once you are uploading data within your S3 bucket, it is continually getting scanned. The fact that the scanning occurs within the AWS account means data never leaves your AWS account, which is also a good security feature. It is real-time, and you can carry out retroactive scans as well. You can even have it API-driven, so before uploading the file to the S3 bucket, you can have it scanned first, before it is being written.

"Antivirus for Amazon S3 has positively impacted my organization by increasing security. I have not actually had any files come back as being insecure, but that is because I have also manually checked the files to make sure that they are secure, and they are. If there was insecure data, I would think that this would pick it up. I have not seen the benefit yet, but that is purely because the data I have been using is already secure. I suppose other organizations which are maybe trying to meet audit requirements would benefit from having this tool because the data is continually being scanned, which would also help audits.."

Verified user

Cloud Ops Lead at a tech vendor with 10,001+ employees

Read full review

“Antivirus for Amazon S3 offers several best features, including automatic malware scanning. The core feature automatically scans files when they are uploaded to S3, detecting viruses, ransomware, Trojans, and other threats. When working with trusted inputs, user uploads, third-party data, and event-driven and real-time processing, the service provides object tagging and metadata-based decisions, automated responses, multiple scanning engines, visibility logging and integration, fully managed and scalable infrastructure, flexible scanning modes, and compliance with security standards such as ISO 27001 and SOC 2 for secure data injected into pipelines.

The two features I find most valuable in Antivirus for Amazon S3 are event-driven scanning and object tagging. Event-driven scanning stands out because it makes the entire workflow real-time and automatic. As soon as a file is uploaded to S3, it gets scanned without any manual trigger. This is critical in production because it ensures no untrusted files sit around waiting to be processed; threats are handled immediately. Object tagging is equally important because it simplifies downstream decisions. Instead of tightly coupling services, we rely on tags such as 'clean' and 'infected'. For example, only files tagged as 'safe' are picked up by processing jobs. This approach keeps the jobs loosely coupled and easy to scale.

Antivirus scanning has a clear positive impact on security, automation, and developer velocity in my organization. From a security standpoint, it has eliminated the risk of malicious files entering downstream systems. Before this implementation, uploaded files were a blind spot. Now we ensure a restricted trust boundary where only scanned and verified files are allowed to move forward. We saw a reduction in security incidents related to file uploads because threats were stopped at injection. This helps us enforce a zero-trust approach for all external data. From a reliability perspective, failed scans default to untrusted, so nothing slips through..”

Janindra Janekumaradi

configuration and management deployment at a tech vendor with 10,001+ employees

Read full review

Other Solutions Considered

"My advice to others looking into using Antivirus for Amazon S3 is that it is absolutely essential; there are options like MetaDefender, Bucket AV, and Amazon GuardDuty to consider, but it's a no-brainer to have antivirus on it when you're thinking about exposing S3 endpoints externally.."

Kalpesh Potghante
Senior Manager at Deloitte

Read full review

"Before choosing Antivirus for Amazon S3, I did not evaluate other options, and that is just because I was using S3 buckets within AWS. I wanted to use their own integrated solution so that it would work with their shared security responsibility model. I could have potentially spun up a container and then deployed a custom solution, but I did not want to do that because it would have taken too much time. The benefit here was that because it is Amazon-managed, it is a lot quicker to get it going.."

Verified user
Cloud Ops Lead at a tech vendor with 10,001+ employees

Read full review

ROI

Real user quotes about their ROI:

"I have seen a return on investment with Antivirus for Amazon S3; while it is a little too early to see the overall impact, detecting 200 plus malware in a month is a good sign of our improved security posture.."

Kalpesh Potghante
Senior Manager at Deloitte

Read full review

"I have definitely seen a return on investment with Antivirus for Amazon S3, including fewer employees needed and time saved. There was an audit system going through those S3 bucket objects, allowing us to directly detect whether there is any threat on those S3 ones coming from third parties.."

AmitSharma3
DevOps Engineer at a tech vendor with 1,001-5,000 employees

Read full review

"I have not seen a return on investment yet as I have not had any insecure data within my cloud account, and because of that, there has not been anything flagged as being insecure. The price of security is really significant, as if you do not have security, the cost of it is much greater than the cost of you actually doing it. You would always hope that you would never have a security issue, so peace of mind is really the main benefit here. Organizations could definitely be helped in their audit processes from using this tool, which alone would save a lot of time and thus money for organizations.."

Verified user

Cloud Ops Lead at a tech vendor with 10,001+ employees

Read full review

Use Case

"I mainly use Antivirus for Amazon S3 for native AWS and Amazon GuardDuty Malware Protection on the S3. I also use it as a third-party marketplace app and as an open-source and DIY solution. These are the main ways I have been using it.."

Abdulsalam Abdulsalam
Security Engineer at SeaLife

Read full review

"My primary use case for Antivirus for Amazon S3 is to secure uploaded files before they are consumed by downstream systems. For example, one workflow involves users uploading documents such as PDFs or images to an S3 bucket via web applications. Since all these files come from external resources, we treat them as untrusted. When a file is uploaded to S3, it triggers an event notification that invokes an AWS Lambda function. The Lambda pulls the objects and scans them using an antivirus engine such as ClamAV. If the file is clean, the tag is set to safe, and it is moved to a processed bucket where downstream services can access it. If it is infected, we quarantine the file in a separate bucket and trigger alerts via SNS and Slack for visibility.."

Janindra Janekumaradi
configuration and management deployment at a tech vendor with 10,001+ employees

Read full review

"My main use case for Antivirus for Amazon S3 is that S3 objects are generally uploaded to the cloud by different clients, and those S3 objects are being consumed by our ECM products.

We upload all the codes of our Lambda functions to S3 because they are large in volume. It may happen that our SCA tools and node modules that are getting uploaded may have vulnerable content or objectionable content, so we use Antivirus for Amazon S3 for scanning them.."

AmitSharma3
DevOps Engineer at a tech vendor with 1,001-5,000 employees

Read full review

"My main use case for Antivirus for Amazon S3 is to automatically scan objects as soon as they're uploaded into S3 buckets. It's mostly used in buckets where files are uploaded by external users or applications, such as documents, reports, or data files. We use it to ensure that no virus or anything affects the integrity of our system.

"I have used Antivirus for Amazon S3 to directly protect our S3 buckets and our entire AWS infrastructure from any malicious files which may pose a threat to our infrastructure. We actively use it for user-uploaded content for one of our applications which requires users to upload content and applications or files. For a dev team, they may also use data ingestion pipelines where files come from external sources. This ensures that infected or suspicious files are detected before they are processed further, and we do not need to check these malicious files on our own.."

Karan Saini
Dev Ops Engineer at a construction company with 11-50 employees

Read full review

"My main use case for Antivirus for Amazon S3 is to utilize an S3 bucket to put static content in, as part of a web app proof of concept that I have been running, and also user content generated from the website. Sometimes I back that up and store it in S3. Using Antivirus for Amazon S3 is really about performing those automated security scans to make sure that the data that is being stored is secure.

"A quick specific example of how I use Antivirus for Amazon S3 in my workflow is for storing static content for a website I have been running, which is a proof of concept blogging website. For example, I am storing images for the blog in S3. Additionally, I carried out a survey on my blog and website that generated user responses, which then get stored in S3. When these objects get stored there, the automatic antivirus scanning, which is deployed on AWS Fargate, gets triggered to make sure that the data being uploaded is indeed secure.."

Verified user

Cloud Ops Lead at a tech vendor with 10,001+ employees

Read full review

"Antivirus for Amazon S3 ensures that all files uploaded to S3 buckets are scanned for malware before they are accessed by applications and end users. This is especially important for customer-facing applications where users upload files such as documents, images, or reports.

"In day-to-day operations, whenever a file is uploaded to an S3 bucket, it triggers an automated scanning process. Antivirus for Amazon S3 scans the file in real-time and based on the result, we either allow the file, quarantine it, or block access if it is malicious.

"For example, in one implementation, I integrated S3 antivirus scanning with our security monitoring system. When an infected file is detected, an alert is generated and the file is automatically isolated. My team then reviews the alert, validates the threat, and ensures that no downstream systems are impacted. This process has significantly reduced the risk of malware entering our environment and improved the overall data security, especially for cloud-hosted applications.."

Vibin Thomas
Team Lead, Technical Content Security at Valuepoint Systems

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.

"My experience with pricing, setup cost, and licensing is that it really is appealing, priced at an optimal point of view, where it feels practically free.."

Kalpesh Potghante

Senior Manager at Deloitte

Read full review

"My experience with pricing, setup cost, and licensing when using Antivirus for Amazon S3 was good, as we were in a POC model to adopt it, and the billing is taken care of by a different team.."

AmitSharma3

DevOps Engineer at a tech vendor with 1,001-5,000 employees

Read full review

Customer Service and Support

"The customer support for Antivirus for Amazon S3 is top notch as we have a golden standard and receive immediate support responses whenever we have any issues.."

AmitSharma3
DevOps Engineer at a tech vendor with 1,001-5,000 employees

Read full review

"Customer support for Antivirus for Amazon S3 gets a ten out of ten. It is Amazon enterprise support if my organization has it, so it ties into that. There are no issues from a customer support perspective.."

Verified user
Cloud Ops Lead at a tech vendor with 10,001+ employees

Read full review

"I have not had a need to contact customer support many times, but during the weekdays, they have been fairly available to us, and in the initial days during the 30-day trial period, we received email support and could contact their expert when required while setting it up, so overall, I'm pleased with the basic support model provided.."

Kalpesh Potghante
Senior Manager at Deloitte

Read full review

Other Advice

"My advice to others looking into using Antivirus for Amazon S3 is that it is something every company needs to try or every engineer that has something on the public cloud or private cloud. I would rate this solution an 8 out of 10.."

Abdulsalam Abdulsalam
Security Engineer at SeaLife

Read full review

"I would highly recommend Antivirus for Amazon S3 to any organization that handles external file uploads or sensitive data in Amazon S3. My review rating for this product is nine.."

Karan Saini
Dev Ops Engineer at a construction company with 11-50 employees

Read full review

"I rate Antivirus for Amazon S3 an eight on a scale of one to ten. I gave it an eight because with the overall scope, I think it is still new, and Antivirus for Amazon S3 will improve over time and absorb more features.

My advice to others looking into using Antivirus for Amazon S3 is to go and use it, so you won't know until you actually use it.

I have additional thoughts about Antivirus for Amazon S3, noting that a lot of vendors are joining in, so we will definitely see rich features. My overall rating for this product is eight out of ten.."

AmitSharma3
DevOps Engineer at a tech vendor with 1,001-5,000 employees

Read full review

"I would recommend Antivirus for Amazon S3 to others looking into using it because it is very easy to set up from the perspective that it is already in AWS. You just have to have some initial development time to write the code to deploy it. After that, there is not too much management unless troubleshooting is needed. I would think most people would not be using a custom solution, so this is much better than not having something.

"I rate Antivirus for Amazon S3 a nine out of ten. I give it a nine because it is a very good tool that leads to peace of mind, but it is a bit complicated to use, a bit difficult to troubleshoot, and also a bit difficult to consolidate the data in CloudWatch to see all the different log streams that are generated.."

Verified user
Cloud Ops Lead at a tech vendor with 10,001+ employees

Read full review

"One important point to add is that the workflow with Antivirus for Amazon S3 has significantly improved our security posture without slowing down development. Before implementing antivirus scanning, there was always a risk of malicious files being consumed by downstream services. By automatically scanning at the S3 level, we created a clear trust boundary where only verified files could move forward.

My advice to others looking into Antivirus for Amazon S3 is to design it as part of your pipeline from day one, not as an afterthought. First, treat all uploaded files as untrusted and enforce a clear flow. Scan immediately at upload and only allow clean files to move forward to avoid a security gap later. Second, keep the architecture simple and event-driven. Third, plan for scale early, especially for large files. Finally, invest in monitoring and failure handling. Ensure failed scans default to untrusted and set up alerts so nothing slips through silently. I would rate my overall experience with Antivirus for Amazon S3 as an eight out of ten.."

Janindra Janekumaradi
configuration and management deployment at a tech vendor with 10,001+ employees

Read full review

"Antivirus for Amazon S3 plays a critical role in our overall layered security strategy. It acts as a key control point at the storage layer, ensuring that any file entering our cloud environment is validated before it is used by applications or shared with users. I integrate it with other security solutions such as SIM, access control policies, and network security tools to create a defense-in-depth approach. This helps us to not only detect malware but also correlate threats across different layers of our infrastructure.

"Additionally, it supports compliance requirements by ensuring that all stored data is scanned and secure, which is especially important for industries handling sensitive data. Overall, it fits seamlessly into our cloud security architecture by providing automated protection, improving visibility, and reducing the risk of

malware propagation across systems.

“Additionally, my advice is to focus on proper integration and automation from the beginning. The real value of Antivirus for Amazon S3 comes when it is fully integrated with services such as S3 event triggers, Lambda, and your security monitoring or SIM platform. I would also recommend defining clear workflows for how to handle infected files, whether to quarantine, delete, or alert, so your response process is consistent and efficient. Another important point is to monitor and tune the solution regularly, especially to reduce false positives and improve detection accuracy over time. Lastly, ensure it is aligned with your overall security strategy and compliance requirements rather than using it as a stand-alone solution. When implemented correctly, it becomes a very effective layer in a defense-in-depth approach. I would rate this solution an 8 out of 10 overall..”

Vibin Thomas
Team Lead, Technical Content Security at Valuepoint Systems

Read full review

Top Industries

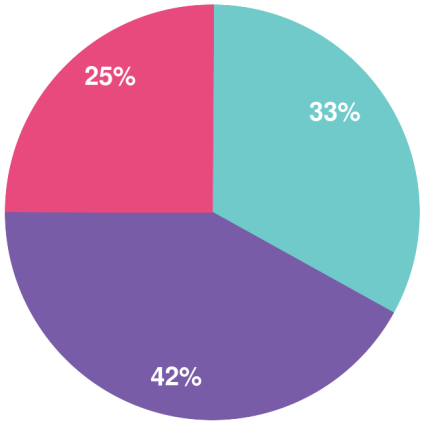
by visitors reading reviews

Construction Company	33%
Comms Service Provider	10%
Manufacturing Company	8%
Healthcare Company	7%

Company Size

by reviewers

by visitors reading reviews



Large Enterprise Midsize Enterprise Small Business

About this buyer's guide

Thanks for downloading this PeerSpot report.

The summaries, overviews and recaps in this report are all based on real user feedback and reviews collected by PeerSpot's team. Every reviewer on PeerSpot has been authenticated with our triple authentication process. This is done to ensure that every review provided is an unbiased review from a real user.

Get a custom version of this report... Personalized for you!

Please note that this is a generic report based on reviews and opinions from the collective PeerSpot community. We offer a customized report of solutions recommended for you based on:

- Your industry
- Company size
- Which solutions you're already considering

The customized report will include recommendations for you based on what other people like you are using and researching.

Answer a few questions in our short wizard to get your customized report.
Get your personalized report here

About PeerSpot

PeerSpot is the leading review site for software running on AWS and other platforms. We created PeerSpot to provide a trusted platform to share information about software, applications, and services. Since 2012, over 22 million people have used PeerSpot to choose the right software for their business.

PeerSpot helps tech professionals by providing:

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

Use PeerSpot to:

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

Join PeerSpot to connect with peers to help you:

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

Visit PeerSpot: www.peerspot.com

PeerSpot

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

reports@peerspot.com

+1 646.328.1944