



Fortinet FortiSandbox

Reviews, tips, and advice from real users



Powered by  **PeerSpot**

Contents

Product Recap..... 3 - 4

Valuable Features..... 5 - 9

Other Solutions Considered..... 10 - 11

ROI..... 12

Use Case..... 13 - 15

Setup..... 16 - 19

Customer Service and Support..... 20 - 22

Other Advice..... 23 - 26

Trends..... 27 - 28

About PeerSpot..... 29 - 30

Product Recap



Fortinet FortiSandbox

Fortinet FortiSandbox Recap

Fortinet FortiSandbox is a behavior-based threat detection solution that prevents and detects malicious code in files transferred within the organization. It is integrated with FortiGate firewalls and FortiMail for threat protection and can be used for monitoring and reporting. The solution inspects files in a virtual environment with different types of virtual machines and can block or quarantine files based on their score.

The most valuable features include dynamic behavior analysis, manual scan features, easy management and configuration, fast scanning, scalability, customization, and ICAP protocol. The solution is cost-effective and faster than other sandbox solutions, with a good user interface.

Valuable Features

Excerpts from real customer reviews on PeerSpot:



“The adapter is beneficial as it allows integration with various devices, not just Fortinet.”



Abdelhamid Saber

Senior Security & Infra Technology Systems Engineer at BARQ Systems



“The most valuable features for me when it comes to Fortinet FortiSandbox are the integrity of the Sandbox and the power of the analyzing tool of the solution.”



Kiarash Heydari

Information security manager at asa com



“It is an easily scalable solution.”



ImranShaikh

Assistant Vice President, PreSales at Netcore Cloud



“The main benefit of Fortinet FortiSandbox is that it allows organizations to detect and prevent unknown threats from entering an infrastructure.”



Reviewer7009881

Independent Consultant



“The solution extracts an attached file before reaching the user and notifies the user if there's something malicious in the attachment received along with an email.”



Marvin Reyes

IT Manager-Infrastructure at Southstar Drug



“The most valuable feature of the solution is that the performance it offers to users is good, making it useful for us in our company.”



Vishnu Gollapudi

Student at KL University



“Fortinet FortiSandbox's most valuable feature is the security it provides against threats, such as ransomware. Additionally, it integrates well with APIs.”



AANKITGUPTAA

Consultant at Pi DATACENTERS

What users had to say about valuable features:

“Currently, there isn't a standout feature. We use Fortinet FortiSandbox for scanning files such as attachments, and we have not faced any issues so far. Up to now, it is performing well..”

Mohammed Hattari

System admin at Environment Fund

[Read full review](#) 

“ The real-time analysis capability of FortiSandbox is beneficial for email analysis, but it's not practical for real-time web traffic analysis because users won't wait for the FortiSandbox to complete its analysis before accessing content. .”

Verified user

CEO at a tech services company with 1-10 employees

[Read full review](#) 

“The most valuable features of the product include components like CDR, greylisting, sandboxing, attachment detection in sandboxing, DLP fingerprinting, and the redirect option..”

ImranShaikh

Assistant Vice President, PreSales at Netcore Cloud

[Read full review](#) 

“The most valuable feature of Fortinet FortiSandbox is its ability to be integrated with email infrastructure, like FortiMail, with a blocking mode option, which means that FortiSandbox not only allows the detection of some malicious objects in emails but also helps block them to prevent end users from receiving from malicious emails..”

Reviewer7009881

Independent Consultant

[Read full review](#) 

“FortiSandbox analyzes the behavior of processes in a sandbox environment, which is useful for threat hunting. The solution has an excellent standard configuration, and you can prioritize the types of files of VMs you want to analyze. It also integrates seamlessly with other Fortinet solutions, like FortiGate, FortiMail, and FortiEMS. .”

Bruno Moreira

Network Security Consultant at SigmaTelecom

[Read full review](#) 

“The integration is easy with other Fortinet products like FortiMail. The technology of sandboxing FortiSandbox can cover it.

Fortinet FortiSandbox has the capability for manual analysis' Unlike its competitors, FortiSandbox offers functionalities such as banning, sniffing, and analyzing traffic in the network. It can connect as a bandwidth analyzer and provide analytics on the network traffic. It's not limited to just sandboxing; it can also operate at the endpoint, firewall, or gateway levels to submit files for analysis and monitor network traffic for analysts..”

Verified user

Security Technical Manager at a tech services company with 51-200 employees

[Read full review](#) 

Other Solutions Considered

“We use different solutions depending on the client's requirements. Sometimes we implement Palo Alto. We need to discuss it with the client and select the product that's appropriate for their use case and environment..”

Verified user

Senior Network Engineer at a tech services company with 1,001-5,000 employees

[Read full review](#) 

“I have used Stormshield in the past. That was a long time ago. We now only use Fortinet for security. Fortinet, in comparison, is easy to configure. Stormshield is also a smaller solution than Fortinet. It's technically more affordable, s Fortinet is more expensive, however, Fortinet is a bigger more technical option..”

Janusz Białowas

Network and Server Engineer at AMiFN

[Read full review](#) 

“Kaspersky, FireEye, and Trend Micro were the solutions I used in the past. Kaspersky, FireEye, and Trend Micro were the solutions I used in the past. I cannot compare the solutions I have used in the past with Fortinet FortiSandbox and comment on which one was the best solution I used since the use of each solution depends on the use cases and Infrastructures. The main advantage of Fortinet FortiSandbox is that it is a part of Fortinet Security Fabric, meaning Fortinet has its own security framework. It is really easy to deploy FortiSandbox and integrate with other Fortinet solutions. Suppose your company has a Fortinet stack or technologies across your network or infrastructure for endpoint protection or network protection. I think Fortinet FortiSandbox would be the easiest choice. I cannot say that Fortinet FortiSandbox is better than Kaspersky, FireEye, or Trend Micro..”

Reviewer7009881

Independent Consultant

[Read full review](#) 

ROI

Real user quotes about their ROI:

“It is a problem task to prove the ROI of any security solution. I saw several cases where FortiSandbox was able to detect some zero-day ransomware attacks at a time when there were no solutions, like FortiSandbox, making it easy for the ransomware attack to be successful. Dealing with a successful ransomware attack would cost a lot of money..”

Reviewer7009881

Independent Consultant

[Read full review](#) 

“Fortinet FortiSandbox saves a lot of money for its users since if an attack happens in your environment, the loss is infinite, especially in terms of the brand value and laws of data. In terms of ROI, the tools safeguard the data and brand value of the company. The percentage of the ROI can vary from company to company. If the product prevents an attack on a small or medium-sized business, then the ROI part will have a different implication in terms of numbers. If the product prevents an attack on an enterprise-sized company, the ROI part will have a different implication in terms of numbers. .”

ImranShaikh

Assistant Vice President, PreSales at Netcore Cloud

[Read full review](#) 

Use Case

“We use Fortinet FortiSandbox for malware. Fortinet FortiSandbox is used before entering the firewall to extract any file and check for malicious activity..”

Marvin Reyes

IT Manager-Infrastructure at Southstar Drug

[Read full review](#) 

“We use this solution to stay updated on the latest vulnerabilities and attacks. It acts as a database for Fortinet customers to keep their equipment safe and secure..”

Soufiane Bouha

Network Security Engineer at MTDS

[Read full review](#) 

“We use FortiSandbox for scanning files and images that pass through our networks. It integrates with different devices, such as five adapters and other Fortinet devices..”

Abdelhamid Saber

Senior Security & Infra Technology Systems Engineer at BARQ Systems

[Read full review](#) 

“The company came to us and provided a proof of concept (POC) for six or seven months for testing the machine and evaluating how we can use Fortinet FortiSandbox. Also, we use FortiSandbox for scanning files, like attachments..”

Mohammed Hattari

System admin at Environment Fund

[Read full review](#) 

“We use Fortinet FortiSandbox for malware analysis, seamlessly integrating with various solutions such as FortiGate, FortiMail for Mail Security, FortiWeb, and other endpoints. FortiSandbox also supports ICAP integration with FortiWeb, enhancing its capabilities. These integrations can be configured within FortiSandbox, either internally or externally. Additionally, FortiSandbox offers integration with Exchange as an adapter..”

Verified user

Security Technical Manager at a tech services company with 51-200 employees

[Read full review](#) 

“We implemented FortiSandbox in three main steps: planning the infrastructure and topology, setting up dedicated Internet access for the sandbox, and configuring manual uploading and email forwarding. For email communication, we used either FortiMail or BCC/force mirroring solutions. FortiSandbox has successfully identified and blocked email attachments containing threats. .”

Verified user

CEO at a tech services company with 1-10 employees

[Read full review](#) 

Setup

The setup process involves configuring and preparing the product or service for use, which may include tasks such as installation, account creation, initial configuration, and troubleshooting any issues that may arise. Below you can find real user quotes about the setup process.

“The initial setup of Fortinet was easy, more so than other products. Even though I'm not directly involved, it has been very easy to work with Fortinet, especially compared to other solutions..”

Mohammed Hattari

System admin at Environment Fund

[Read full review](#) 

“A network security engineer can deploy the solution. The organization's IT department manages administration, including application and network security. Multiple administrators may use FortiSandbox, each with their front-end interface for managing it..”

Verified user

Security Technical Manager at a tech services company with 51-200 employees

[Read full review](#) 

“We have the support to set it up. It took a few months to deploy it. We integrate the solution and the support takes care of the solution after that. Almost three to four people are required for the maintenance.

.”

Mohamed -Adel

IT Specialist at IPIC

[Read full review](#) 

“The product is easy to deploy.

The product can be deployed in 15 days.

Two or three people from our company are involved in the deployment, implementation, and configuration process. .”

ImranShaikh

Assistant Vice President, PreSales at Netcore Cloud

[Read full review](#) 

“The solution is not complex as they are already included in Fortinet. There is a special solution for sandboxing, but it increases the level of security. In that version, you can get more from that solution and more efficiency in using sandboxing.

The initial setup is easy because I have been working with Juniper, and they have the same interface. The graphic interface is friendly and it is intuitive. For me, it is easy to configure..”

Vinicius Borges

[Read full review](#) 

IT Project Management at a energy/utilities company with 11-50 employees

“The initial setup phase of Fortinet FortiSandbox was pretty straightforward because, in my case, I worked with the physical appliances. According to the documentation, the setup phase for virtual appliances would be exactly the same as for physical appliances. You just deploy the box and then configure it, after which you create some integrations with FortiMail and other systems, which may take less than an hour.

The solution is deployed on an on-premises model.

The solution can be deployed in an hour or even less in the easiest scenarios. In the not-so-easy scenarios, the deployment phase for the solution may take a day or two. Some of my company's customers want to integrate Fortinet FortiSandbox with FortiMail and other tools, so it involves multiple integration points. The purpose of integrating Fortinet FortiSandbox with other tools may be to simultaneously monitor network or email traffic and use some customized images for virtual machines, which does take time. There is a need to perform fine-tuning in the solution to set up detection capabilities and some mechanisms..”

Reviewer7009881

[Read full review](#) 

Independent Consultant

Customer Service and Support

“As of now, I've primarily been in contact with the consultants for support and have only needed one ticket with Fortinet. I have no substantial experience with Fortinet's direct technical support..”

Mohammed Hattari

System admin at Environment Fund

[Read full review](#) 

“Technical support has been pretty good. I know they respond every time. It just takes a few hours. It doesn't take too much time to respond. They're helpful and you can count on them..”

Verified user

Architect of solutions at a comms service provider with 11-50 employees

[Read full review](#) 

“We have great support from Fortinet. We have our own research partner who can assist us with configuration and getting to know the product. They're easily available to inform us about new features, new rollouts, and the new operating system in the FortiOS. .”

Verified user

Principal Cyber Security Architect at a comms service provider with 5,001-10,000 employees

[Read full review](#) 

“They are very responsive. At first, I had interacted with only the Greece branch of Fortinet, which has only pre-sales engineers, not the support engineers, and they were very helpful. For the last two and a half years, we have a contract with a dedicated team for support. They're getting bigger, better, and greater. .”

Dikeos Davakis

ICT Manager at Nic. J. Theocarakis

[Read full review](#) 

“Whenever we reach out to Fortinet, they give a response in time. Till now, we have had positive interactions.

We connect with FortiGate through qualified vendors, especially regarding SLA and responsiveness..”

Soufiane Bouha

Network Security Engineer at MTDS

[Read full review](#) 

“Support has been mostly helpful.

I have a contact from Fortinet support and my contact is very nice. I use it three to five times a year and they've mostly;y been able to support me and answer my questions.

We do pay for support and they do provide us with help and with patches, et cetera, to help with firmware and updates and any security items. .”

Janusz Białowas

Network and Server Engineer at AMiFN

[Read full review](#) 

Other Advice

“If you're using Fortinet, it's best to use the solution when using FortiGate antivirus because it's all connected and easy to manage.

Overall, I rate Fortinet FortiSandbox an eight out of ten..”

Marvin Reyes

IT Manager-Infrastructure at Southstar Drug

[Read full review](#) 

“If the customer's operating system is supported, there's no need for a custom package. It's straightforward. If a custom operating system is required, it will take longer due to the need for package customization.

Overall, I rate the solution an eight out of ten..”

Verified user

Security Technical Manager at a tech services company with 51-200 employees

[Read full review](#) 

“I recommend using FortiSandbox, especially if your environment relies on [FortiGate](#) devices or is integrated with Fortinet. It ensures better compatibility.

I'd rate the solution nine out of ten..”

Abdelhamid Saber

Senior Security & Infra Technology Systems Engineer at BARQ Systems

[Read full review](#) 

“If a company has some Fortinet equipment in its environment already, then Fortinet FortiSandbox would be the best choice for them. If a company wants to go for the deployment of some other solution for all their infrastructures, then it would be good to analyze the integration and detection capabilities.

I rate the overall solution a nine out of ten..”

Reviewer7009881

Independent Consultant

[Read full review](#) 


“Though I haven't worked with Fortinet FortiSandbox, it is a good solution based on the opinion of one of my colleagues who has worked with it. Fortinet FortiSandbox can be deployed on a cloud or on-premises.

I recommend the solution to those who plan to use it. Fortinet FortiSandbox is a good security option for those who plan to use it.

The overall solution is an eight to nine out of ten..”

Vishnu Gollapudi

Student at KL University

[Read full review](#) 

“I would describe Fortinet FortiSandbox, which has been deployed within our company's network for threat detection, as a proactive solution with multiple functionalities. A few of the functionalities of the product include areas like sandboxing, CDR, pattern-reading, and detection ratio, which are very good.

I rate the product's effectiveness in dealing with zero-day threats a seven to eight out of ten, where ten means it is the most effective product for dealing with zero-day threats.

As of now, Fortinet FortiSandbox is not integrated with other Fortinet solutions to improve our company's security posture. The tool is integrated with our own existing email security gateway to use anti-spam and anti-virus features.

The tool should have more ability to customize from the reporting point of view. The tool should be able to provide more slicing and dicing in data. The users of the product should try to know about threat chains with the help of the tool's MSPs so that they know the outcome of a threat that may enter their networks. In the MSP model, it would be good if the aforementioned area gets integrated.

The reporting and alerting capabilities of the product have helped our company's security area since the tool provides good and deep-dive reports, which include

proper reasoning for certain actions that were taken. The report will explain why it blocked or did not block certain aspects. There are detailed reports in terms of the logs that the tool provides its users. The tools also provide details on the areas that were quarantined. In general, the tool provides a very detailed report.

The product is easy to maintain since my company gets proper support from Fortinet.

In my company, there are many use cases to describe scenarios where the product prevented or mitigated a breach or an attack. My company operates as a managed service provider for Fortinet, and many of our customers use Fortinet FortiSandbox. When my company receives any attacks via links or attachments, [FortiMail](#) blocks such emails.

I suggest others consider whether they plan to buy a solution from a security company. I will see whether the tool I use for sandboxing is from a security company or not. I will consider the catch rate of the product. I will also consider the other solutions that the vendor can bring in for me that can improve and secure my company's security posture while being easy to use and implement.

I will consider whether the vendor who offers our company sandboxing features has a security background. I will look into whether the solution is interoperable or not. There should be interoperability if I need to deploy some other solution as well, like a [DLP](#) or a firewall.

I rate the overall tool a seven out of ten..”

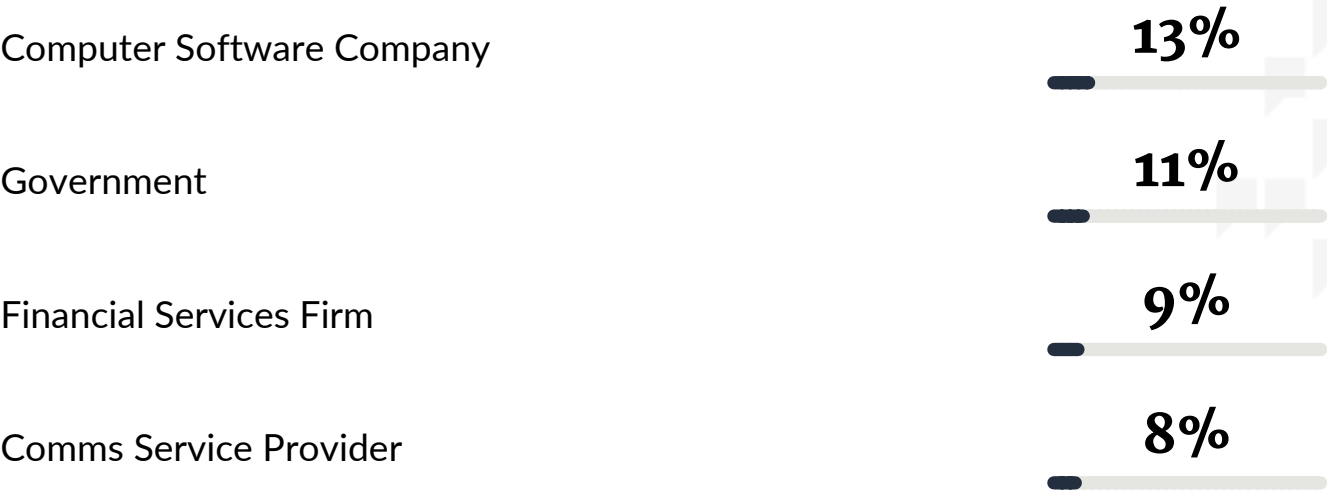
ImranShaikh

Assistant Vice President, PreSales at Netcore Cloud

[Read full review](#) 

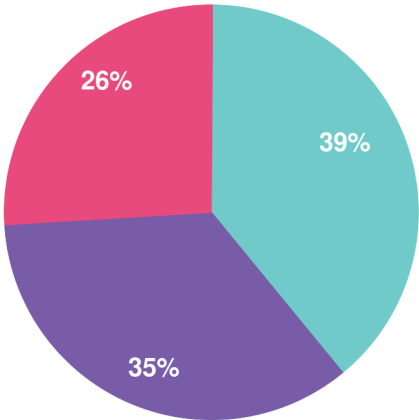
Top Industries

by visitors reading reviews

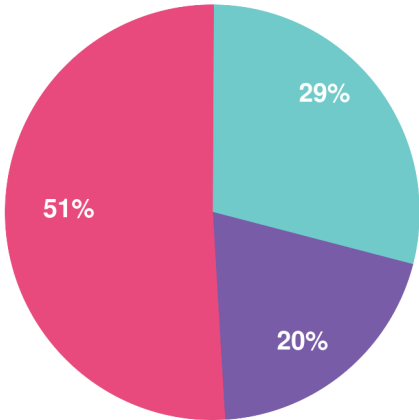


Company Size

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 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