aws marketplace

ReversingLabs

Reviews, tips, and advice from real users






Powered by PeerSpot

Contents

Product Recap

ReversingLabs

ReversingLabs Recap

ReversingLabs is the trusted authority in software and file security. We provide the modern cybersecurity platform to verify and deliver safe binaries. Trusted by the Fortune 500 and leading cybersecurity vendors, the ReversingLabs Titanium Platform® powers the software supply chain and file security insights, tracking over 35 billion files daily with the ability to deconstruct full software binaries in seconds to minutes. Only ReversingLabs provides that final exam to determine whether a single file or full software binary presents a risk to your organization and your customers.

RL - Trust Delivered.

https://www.reversinglabs.com

Valuable Features

Excerpts from real customer reviews on PeerSpot:

"The automated static analysis of malware is the most valuable feature. Its detection abilities are very good. It hits all of the different platforms out there, platforms that see the items in the wild."

Tim Craig

Forensic Lead, Global Security Fusion Center at a insurance company with 10,001+ employees

"It offers reports on a great many more file types than the other analysis solutions we have. It can give us a more in-depth analysis and better reporting on a larger number of file types. It also gives us a more comprehensive score on a number of things as well, and that's why we're using it as a front-end filter. It gives us more information... It's valuable because of its depth of information, as well as the breadth it gives us. There aren't a lot of tools that cover all of the different file types."

Verified user

Information Security Engineer IV at a financial services firm with 1,001-5,000 employees

"As far as the malware repository is concerned, it's extensive. It's a good source for finding samples, where we are unable to find them on other channels or by leveraging other sources."

Verified user

CSO - Information Security at a financial services firm with 1,001-5,000 employees

"ReversingLabs has a large sample size."

Jesse Harris

Principal Solutions Architect at a tech vendor with 1,001-5,000 employees

What users had to say about valuable features:

"The automated static analysis of malware is the most valuable feature. Its detection abilities are very good. It hits all of the different platforms out there, platforms that see the items in the wild.

Also, the solution's object and file analysis provide us with actionable insights.

Its malware and goodware repository is very good. It's very robust. It gets all of the different repositories that are out there that do analysis and brings them under one roof where we can statically analyze for those indicators of compromise and look at them more deeply. If we need to go deeper into things, we can do that.."

Tim Craig

Forensic Lead, Global Security Fusion Center at a insurance company with 10,001+ employees

Read full review

“We are primarily using it for its static analysis capabilities. It is valuable because it offers reports on a great many more file types than the other analysis solutions we have. It can give us a more in-depth analysis and better reporting on a larger number of file types. It also gives us a more comprehensive score on a number of things as well, and that's why we're using it as a front-end filter. It gives us more information, and then we use that information to decide whether or not we want to send it on and do further analysis. It's valuable because of its depth of information, as well as the breadth it gives us. There aren't a lot of tools that cover all of the different file types.

While we have not extensively tested the detection, it has detected everything that we've thrown at it that we've known is malicious. From the numbers they've given us, the solution's malware and goodware repository seems huge.

It easily integrates with our SIEM, Splunk..”

Verified user

Information Security Engineer IV at a financial services firm with 1,001-5,000 employees

Read full review

"As far as the cloud version is concerned, we mostly leverage the product to retrieve samples, or malicious programs, that we are otherwise unable to find. So, the ability to download programs directly from the platform is of importance to us. Other than that, we mostly leverage the information regarding static analysis.

As far as URLs are concerned, we would use the product as a source to verify whether or not the URL has been flagged as malicious.

As far as static analysis information is concerned, we use most of the information that is available in order to determine whether or not we might be dealing with a malware variant. This includes information that is related to Java rules. This is also related to malware families indicated or specific malicious software variants that are labeled by name. Besides this, packing or unpacking related information is something that we leverage a lot.

As far as the malware repository is concerned, it's extensive. It's a good source for finding samples, where we are unable to find them on other channels or by leveraging other sources.."

Verified user

CSO - Information Security at a financial services firm with 1,001-5,000 employees

Read full review

Other Solutions Considered

"I don't believe they looked into any other products before choosing ReversingLabs. And I've been very satisfied with ReversingLabs. If it isn't broken, why try to fix it?."

Tim Craig

Forensic Lead, Global Security Fusion Center at a insurance company with 10,001+ employees

Read full review

"We evaluated most of the features that we were eventually licensing. That included, for instance, the possibility to download malicious programs from the repository. As far as the static analysis engine was concerned, we ran a very in depth evaluation. We also compared the results of those analyses with information that we had available from other tools. So, there were some quite in-depth technical assessments done before purchasing the solution.."

Verified user

CSO - Information Security at a financial services firm with 1,001-5,000 employees

Read full review

“We had nothing and that's why we went to the Titanium platform. We had nothing in the environment to do such analysis, so it's been a savior in many ways. We had nothing even close to what ReversingLabs does.

Leadership realized we needed something like this because of the turnover of talent and people not having an understanding of malware analysis. We needed some type of reliable solution that would help with at least the static analysis of such items..”

Tim Craig

Forensic Lead, Global Security Fusion Center at a insurance company with 10,001+ employees

Read full review

“We are also using FireEye and Palo Alto. As far as I can tell, the quantity of files that the ReversingLabs solution can process in a day is greater than many of these products. Also, the stability of this product seems to be much higher than some of the other ones that we've had issues with.

- Stability
- reliability
- volume of processing

are the pros.

On the other hand - and this is something of a pro and a con - there's a lot of tooling that we need to build up around the solution to get it to integrate with our existing setup. That's a plus and a minus, in that once we get it integrated, and once we understand all of the interfaces to this product and how best to utilize it, then it becomes a tool that we can extend in our own right. But the con side of it is that it takes all that engineering work, all that understanding, all that effort, and we're not there yet. And we've been doing this for some time. Other tools do not require as much of that sort of effort.

ReversingLabs is going to be one of many things that we use. We don't want a mono-culture here, and we don't want information from just one vendor or one perspective. But we do respect ReversingLabs enough to put them in a very critical role in our infrastructure. We want to analyze pretty much everything that comes into our company, from email attachments to new files that are dropped by Microsoft updates, to files that people save on network drives, and we're going to use ReversingLabs to ingest all of those samples.

ReversingLabs is supplemental for us. It will be a kind of filter before things get to the other solutions..”

Verified user

Information Security Engineer IV at a financial services firm with 1,001-5,000 employees

Read full review

Use Case

“We haven't finished building it out fully but we want to use it as a pre-filter before samples go to anything else for analysis. Things are going to be coming to it and we're going to get a score regarding what ReversingLabs thinks of any file samples and, if it's a score that says it's a high threat level, we'll send it on for further analysis in other automated platforms..”

Verified user

Information Security Engineer IV at a financial services firm with 1,001-5,000 employees

Read full review

“We use it to analyze and pull out any indicators of compromise from malware that we get within the environment. We check to see if those indicators are seen throughout our infrastructure.

We also do some type of open-source intelligence using the platform, at a basic level, dumping emails into it to see if it can parse out any of the URLs and the like. But that part is very basic.

We're basically using it as a "sandbox" for static analysis. It's on-prem. Only certain people have access to it. It's not integrated into our whole environment as of yet. I would like it to be in our plans to do so but, currently, it's not deployed in that manner..”

Tim Craig

Forensic Lead, Global Security Fusion Center at a insurance company with 10,001+ employees

Read full review

“The primary use case is static analysis and retrieval of malware relevant indicators.

We have multiple products in use. As far as the onsite product is concerned, we use the latest version of the product. The other version is a cloud-based solution, so I assume this is always the latest version.

We are not integrating the solution with our bank technologies directly since we are employing the solution in a special infrastructure, which is isolated from the rest of the production network for security reasons. However, we do integrate the solution with a number of other analysis technologies that we use as part of our laboratory infrastructure. As far as this is related, integration is fine.

As far as the static analysis capabilities are concerned, they're used extensively on a daily basis. We've just completed the integration of the cloud-based variant..”

Verified user

CSO - Information Security at a financial services firm with 1,001-5,000 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 was straightforward.

We were able to use the product within a day, then started integrating it in into our own platform. It was mostly access credential-based.."

Verified user

CSO - Information Security at a financial services firm with 1,001-5,000 employees

Read full review

"We have a separate engineering and infrastructure side, so I can't talk about the actual deployment in detail. But I believe that once we set up the environment, we were provided with a VM of the system. But there was more of a connection with our engineering groups to get it deployed within the environment, so we could access it and use it for our analysis.

It only took one guy a couple of days. And it takes just one person to maintain it, again within the engineering team. There are about 35 of us using it, including level-ones, level-threes, and forensics.."

Tim Craig

Forensic Lead, Global Security Fusion Center at a insurance company with 10,001+ employees

Read full review

"This was my first time ever doing something like this, and I was working with a team to do it. The initial setup did seem, to me, to take a while, but I don't have enough perspective to judge how complex or straightforward it was because I've never done anything comparable.

Our deployment has been ongoing for about a year.

Our implementation strategy is to get a number of sources of file samples and hashes onboarded into the ReversingLabs ecosystem, whether it be the APIs or the appliances, including the A1000, and once we do that in development we want to export what we've learned to production.."

Verified user

Information Security Engineer IV at a financial services firm with 1,001-5,000 employees

Read full review

Customer Service and Support

"Their engineering team has been great. In everything that we've done so far with ReversingLabs, they have been very responsive and very helpful on the support side. They're as speedy as they can be.."

Verified user

Information Security Engineer IV at a financial services firm with 1,001-5,000 employees

Read full review

"The product support could be better at times. They are typically okay. They are definitely trying to reach high customer satisfaction. They are also available on a very short notice. Sometimes, the resources that they provide could be of higher quality.."

Verified user

CSO - Information Security at a financial services firm with 1,001-5,000 employees

Read full review

“Their staff has always been responsive and great. I have nothing but great things to say about them. They've been awesome anytime I have a question. I don't have to wait 24 hours for an answer; usually, it's no more than an hour to two hours. And I've never had to escalate an issue.

I've had great relationships with the company. Even if somebody leaves and somebody comes on, they're very responsive. There's rarely a hiccup with their product..”

Tim Craig

Forensic Lead, Global Security Fusion Center at a insurance company with 10,001+ employees

Read full review

Other Advice

“Anything we've pumped at this thing, it seems that it's just fine handling it. That's one of the big reasons we want it to be the funnel that everything comes through first. We want that determination of good, bad, or suspicious. We have complete faith that it can do that for us, and can do it at scale.

It's stellar. I would easily give it a nine out of ten. I've had a great experience with it..”

Verified user
Information Security Engineer IV at a financial services firm with 1,001-5,000 employees

Read full review

“Work with the ReversingLabs team. They're great to work with, and they're willing to help in any way.

The biggest lesson I've learned from using it is that I need to know a heck of a lot more about the solution's power and how we can better integrate it into the environment for all our teams to use.

We don't deploy it in a fashion where it is integrated with our existing security investments as of yet. We are going to look into those integrations in the next few quarters. Right now, it's more of a standalone analysis system that is not hooked up to any of our EDR solutions. We have also not looked into the Threat Summary Dashboards yet. We've had a lot of employee changes and leadership changes. That's one of those things that is on the to-do list, but no one has really sat down and gone over it all..”

Tim Craig
Forensic Lead, Global Security Fusion Center at a insurance company with 10,001+ employees

Read full review

“It's definitely a technical product. Some expertise and experience with malware analysis and anti-malware operations is required. Only purchasing the static analysis parts, as well as the APIs, this typically requires some maturity in the Security Operations Center (in respect to CERTs). If this is not the case, then respective teams should opt for the graphical user interface, which provides more guided support. Other than that, it's a good product.

I would rate it approximately seven and a half to eight. One of the problems is currently that the company offers three different types of products which are very similar to each other. It's not entirely clear during respective discussions how those different products can be truly distinguished from each other. Besides having a graphical user interface and a cloud-based variant, there was originally just one product, which eventually evolved into different directions. Then, it became a series of different products. For the customer, this is not that easy to understand.

The other aspect is, as far as the APIs are concerned, the respective sample scripts are not of very high quality. Some of them are really basic, and that code base should generally be improved.

We are not leveraging the product as part of SOC operations. We use it for contributing to our anti-malware related operations, which is slightly different.

We don't use the solution's threat summary dashboards.

We're not leveraging the whitelist so much, so I can't say much about the goodware..”

Verified user
CSO - Information Security at a financial services firm with 1,001-5,000 employees

Read full review

Top Industries

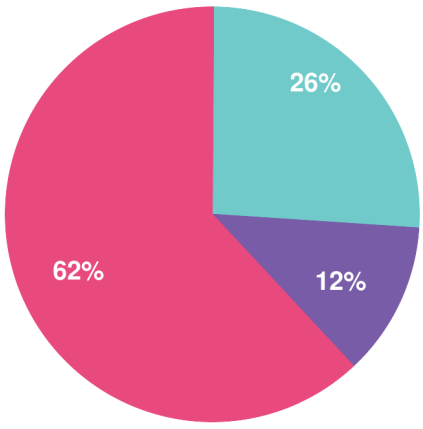
by visitors reading reviews

Computer Software Company	16%
Financial Services Firm	13%
Insurance Company	8%
Manufacturing 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