



**Contrast Security Assess**

# Reviews, tips, and advice from real users



Powered by  **PeerSpot**

# Contents

Product Recap..... 3 - 4

Valuable Features..... 5 - 12

Other Solutions Considered..... 13 - 16

ROI..... 17 - 19

Use Case..... 20 - 22

Setup..... 23 - 27

Customer Service and Support..... 28 - 30

Other Advice..... 31 - 36

Trends..... 37 - 38

About PeerSpot..... 39 - 40

# Product Recap



Contrast Security Assess

# Contrast Security Assess Recap

Contrast Security is the world's leading provider of security technology that enables software applications to protect themselves against cyberattacks, heralding the new era of self-protecting software. Contrast's patented deep security instrumentation is the breakthrough technology that enables highly accurate assessment and always-on protection of an entire application portfolio, without disruptive scanning or expensive security experts. Only Contrast has sensors that work actively inside applications to uncover vulnerabilities, prevent data breaches, and secure the entire enterprise from development, to operations, to production.

# Valuable Features

Excerpts from real customer reviews on PeerSpot:



“Assess has an excellent API interface to pull APIs.”



**ToddMcAlister**

Lead Application and Data Security Engineer at a insurance company with 5,001-10,000 employees



“When we access the application, it continuously monitors and detects vulnerabilities.”



**Mustufa Bhavnagarwala**

CyberRisk Solution Advisor at a consultancy with 10,001+ employees



“The solution is very accurate in identifying vulnerabilities. In cases where we are performing application assessment using Contrast Assess, and also using legacy application security testing tools, Contrast successfully identifies the same vulnerabilities that the other tools have identified but it also identifies significantly more. In addition, it has visibility into application components that other testing methodologies are unaware of.”



**Verified user**

Director of Threat and Vulnerability Management at a consultancy with 10,001+ employees



“I am impressed with the product's identification of alerts and vulnerabilities.”



**Aggelos Karonis**

Senior Manager of Information Security at Kaizen Gaming



“In our most critical applications, we have a deep dive in the code evaluation, which was something we usually did with periodic vulnerability assessments, code reviews, etc. Now, we have real time access to it. It's something that has greatly enhanced our code's quality. We have actually embedded a KPI in regards to the improvement of our code shell. For example, Contrast provides a baseline where libraries and the usability of the code are evaluated, and they produce a score. We always aim to improve that score. On a quarterly basis, we have added this to our KPIs.”



**Aggelos Karonis**

Technical Information Security Team Lead at Kaizen Gaming



“We use the Contrast OSS feature that allows us to look at third-party, open-source software libraries, because it has a cool interface where you can look at all the different libraries. It has some really cool additional features where it gives us how many instances in which something has been used... It tells us it has been used 10 times out of 20 workloads, for example. Then we know for sure that OSS is being used.”



**Ramesh Raja**

Senior Security Architect at a tech services company with 5,001-10,000 employees



“The most valuable feature is the continuous monitoring aspect: the fact that we don't have to wait for scans to complete for the tool to identify vulnerabilities. They're automatically identified through developers' business-as-usual processes.”



**Verified user**

Manager at a consultancy with 10,001+ employees

What users had to say about valuable features:

“When we access the application, it continuously monitors and detects vulnerabilities. Contrast Security Assess detects, even at runtime and in the code part, which file or line of code has the vulnerability..”

**Mustufa Bhavnagarwala**

CyberRisk Solution Advisor at a consultancy with 10,001+ employees

[Read full review](#)

“Contrast Security Assess is one of the first players in this market, so they have experience and customers, especially abroad. Overall, it's a good product. But, again, if you are commercially weak, you remain a single supplier. In any given market with only one supplier, the market cannot function. It is important to have competition, and one should gain market share through flexibility. It will be too late in two years, as many companies claim to be doing IAST. It's like selling there's no Desktop antivirus versus traditional antivirus. Everybody shall do signature-less virus detection. Otherwise, you're out of the market. This scenario is very similar here, especially in the forward applications..”

**Paolo Da Ros**

Founder at a tech services company with self employed

[Read full review](#) 

---

“The solution is very accurate in identifying vulnerabilities. In cases where we are performing application assessment using Contrast Assess, and also using legacy application security testing tools, Contrast successfully identifies the same vulnerabilities that the other tools have identified but it also identifies significantly more. In addition, it has visibility into application components that other testing methodologies are unaware of.

Assess also provides the option of helping developers incorporate security elements while they're writing code. It depends on whether individual developers decide to utilize the information that's provided to them from the solution, but it definitely gives them visibility into more environments. It gives them an opportunity to remediate vulnerabilities well before production deployments..”

**Verified user**

Director of Threat and Vulnerability Management at a consultancy with 10,001+ employees

[Read full review](#) 



“The real-time evaluation and library vulnerability checks are the most valuable features, because we have a code that has been inherited from the past and are trying to optimize it, improve it, and remove what's not needed. In this aspect, we have had many unused libraries. That's one of the key things that we are striving to carve out at this point.

An additional feature that we appreciate is the report associated with PCI. We are Merchant Level 1 due to the number of our transactions, so we use it for test application compliance. We also use the OWASP Top 10 type of reports since it is used by our regulators in some of the markets that we operate in, such as, Portugal and Germany.

The effectiveness of the solution's automation via its instrumentation methodology is very effective and was a very easy integration. It does not get affected by how many reviews we perform in the way that we have designed the release methodologies. So, it has clear visibility over every release that we do, because it is the production code which is being evaluated.

The solution has absolutely helped developers incorporate security elements while they are writing code. The great part about the fixes is they provide a lot of sensory tapes and stuff like what you should avoid to do in order to avoid future occurrences around your code. Even though the initial assessment is being done by a senior, more experienced engineers in our organization, we provide the fixes to more junior staff so they have a visceral marker for what they shouldn't do in the future, so they are receiving a good education from the tool as well..”

**Aggelos Karonis**

Technical Information Security Team Lead at Kaizen Gaming

[Read full review](#) 

“Assess is valuable for several reasons, but time-saving factors are high on the list. Compared to a typical development environment with a SAST tool, Assess saves developer time and reduces the time-to-market. With Assess there is no waiting for a slow static scan to complete. Vulnerability findings are reported during testing and the reported findings are highly accurate, with very few false positives. Other SAST tools often emit a great number of false positives that must be investigated and resolved before the code can be released, consuming the time of developers and the security team chasing invalid vulnerability reports. Assess also provides clear and actionable guidance on how to fix each vulnerability, saving more time.

Assess integrates with a many common tools to generate notifications and tickets, such as JIRA tickets. The result is that application security vulnerabilities can be handled by developers as just another type of bug found during testing. Application security becomes part of the development process rather than a step that is done “after” development. The temptation to skip the security testing step to meet a release deadline is eliminated.

The combination of real-time analysis and accurate vulnerability reports can really accelerate time-to-market. One large customer was even able to eliminate the human signoff before release to production. This customer had a solid DevOps process with automated application testing, but still had the security testing and review process delaying releases. With Assess in their pipeline they were able to automate the release decision. Apps that passed functional tests and reported only vulnerabilities below a certain criticality threshold would be automatically released directly to production. .”

**Verified user**

[Read full review](#) 

Senior Customer Success Manager at a tech company with 201-500 employees

“The most valuable feature is the continuous monitoring aspect: the fact that we don't have to wait for scans to complete for the tool to identify vulnerabilities. They're automatically identified through developers' business-as-usual processes.

The automation of the actual vulnerability identification is great. I would give it a very high rating, given that it requires little of the security team or developers to understand and start reviewing the results that are identified.

The false positive rate is another good feature. It has a very low false positive rate. That means my team, the security team, has to spend less time looking at results and findings, compared to historical, static and dynamic scans where the false positive rate is much higher. From a percentage perspective, somewhere around 90 percent of the time we used to spend has been given back to our team, because the false positive rate with Contrast is less than 5 percent.

In terms of the accuracy of vulnerability identification, so far we've had tens of thousands of issues identified in applications that have historically been scanned by dynamic and static scanning. So far, the large majority of those findings have been true positive. I may have seen just a handful, five or 10, false positives so far, in the scope of tens of thousands. That's a very low rate.

We also use the solution's OSS feature through which we can look at third-party open source software libraries. It is a great tool. We've never had a solution for software composition analysis. It has affected our software development greatly. Since we've never really had a solution for doing software composition, nor have we required fixes for vulnerable third-party libraries, this has changed the way that developers are looking at usage of third-party libraries, upfront. It's changing our model of development and our culture of development to ensure that there is more thought being put into the usage of third-party libraries. The solution is definitely helping developers incorporate security elements while they are writing code. Since we're able to install Assess in Development and QA and all the pre-production environments, developers can start making use of the tool as soon as they have a deployed version of their products. As they code new features and test

those out in their development environment, Contrast is already going to be automatically identifying things at that point. We are identifying issues much earlier in the software development life cycle, which makes it much less costly for developers to fix those findings.

We're saving time and money by fixing software bugs earlier in the software development life cycle. We're saving time on the developers' side, as well as on the security auditors' side..”

**Verified user**

Manager at a consultancy with 10,001+ employees

[Read full review](#) 

# Other Solutions Considered

“I have used SonarQube and GitLab Premium before. We decided to go with Contrast because it has the best price model since it takes into account only the number of applications. It also finds vulnerabilities within minutes of its launch. The product is also developer-friendly..”

**AggelosKaronis**

Senior Manager of Information Security at Kaizen Gaming

[Read full review](#) 

---

“We did not use any other interactive application security testing solutions. There are very few on the market. We did use legacy technologies like DAST and SAST. We still use those technologies in our environment mostly to supplement Contrast or to assess environments that Contrast is not able to assess..”

**Verified user**

Director of Threat and Vulnerability Management at a consultancy with 10,001+ employees

[Read full review](#) 

“We evaluated all of the IAST products that were on the market at the time. It was the most mature product in the space. One vendor had an IAST solution, but it wasn't a fully developed solution; they may not have even had any customers. There was another that had a fairly mature IAST product, but they hadn't done a lot of development in terms of the look and feel. Contrast was a very complete solution. It met all of our technical requirements and it was really the only IAST product that felt like a real product..”

**Verified user**

[Read full review](#) 

Director of Threat and Vulnerability Management at a consultancy with 10,001+ employees

---

“Before choosing Contrast Assess, we looked at Veracode and Checkmarx.

Contrast does things continuously so it's more of an IAST. Checkmarx didn't. Using it, you would have to upload a .war file and then it would do analysis. You would then go back to the portal and see the vulnerabilities there.

It was the same with Veracode. When you take a SAST piece or a DAST piece, you have to have some specific timing in some workflows and then you upload all of the stuff to their portal and wait for results. The results would only come after three days or after five days, depending on how long it takes to scan that specific workflow.

The way the scanning is done is fundamentally different in Contrast compared to how the solutions do it. You just install Contrast on the app server and voilà. Within five minutes you might see some vulnerabilities when you use that application workflow..”

**Ramesh Raja**

[Read full review](#) 

Senior Security Architect at a tech services company with 5,001-10,000 employees

---

“We had an extensive list that we examined. We dove into some portable solutions. We did have some excellent competitors because they gave us a clear indication of what we wanted to do. We examined SonarQube and Veracode, who presented us with a great product, but was not a great fit for us at the time. These solutions gave us the idea of going with something much larger and more broad than just a tool to produce findings. So, many competitors were examined, and we just selected the one who mostly fit our way of doing things.

The main thing to note is the key differentiation between Contrast and everything else we evaluated is the production value range since we had the chance to examine actual requests to our site using our code. Contrast eliminated the competition with their ability to add the live aspects of a request taken. That was something we weren't able to find in other solutions.

Some of the other competitive solutions were more expensive..”

**Aggelos Karonis**

Technical Information Security Team Lead at Kaizen Gaming

[Read full review](#) 

“Prior to to this, we did not have such a solution and relied on other controls.

Our initial thought was that we needed a SAST tool. So, we proceeded with approaching some vendors. What sparked the interest for Contrast is its real-time evaluation of requests from our users and identification of real-time vulnerabilities.

We have now established specific web nodes serving those requests. We get all the feedback from there along with all the vulnerabilities identified. Then, we have a clear dashboard managed by our information security team, which is the first step of evaluation. After that, we proceed with adding those pieces of the vulnerabilities to our software development life cycle.

Prior to using Contrast, we didn't have any visibility. There were no false positives; we had just the emptiness where even false positives would be a good thing. Then, within the first week of having the tool, 80 or 90 vulnerabilities had been identified, which gave us lots to do with minor false positives..”

**Aggelos Karonis**

Technical Information Security Team Lead at Kaizen Gaming

[Read full review](#) 



# ROI

Real user quotes about their ROI:

“From a security team perspective, we're able to free up a lot more time. We spend less time reviewing results and can spend our time elsewhere. Developers have the same thing. They can spend more of their time working on actionable results rather than looking at false positives and waiting for the security team to complete testing on their behalf..”

**Verified user**

Manager at a consultancy with 10,001+ employees

[Read full review](#) 

“We have definitely seen ROI. We have been able to onboard our applications and scan them. The scan is happening continuously, every day, and it does report new findings. We have been able to triage them and fix them, address the defects of the software, even before they were posted to Prod. This will help reduce our attack surface and make our products more secure..”

**Verified user**

Product Security Engineer at a tech services company with 10,001+ employees

[Read full review](#) 

“We expect to see ROI with the architecture team, the infrastructure team, and with the development teams, especially when it comes to how early in our development cycle the vulnerabilities are found and remediated. That plays a big part because the more time it takes to find a software vulnerability, obviously, the more your cost to market will be substantially higher..”

**Ramesh Raja**

Senior Security Architect at a tech services company with 5,001-10,000 employees

[Read full review](#) 

---

“We have seen ROI, but I can't get into specific numbers because those are sensitive to the organization. But some of these applications are key revenue drivers. Contrast's ability to help secure them, even if it is just those applications, gives us a little confidence that they are being looked at in terms of security. That is always going to be a significant return on investment, compared to the other tools that, frankly, weren't driving the progress necessary to secure those applications..”

**Verified user**

Director of Innovation at a tech services company with 1-10 employees

[Read full review](#) 

“The solution has helped save us time and money by fixing software bugs earlier in the SDLC. The code shells and quality improve through missed links and libraries as well as units of extensive code where it's not needed. From many aspects, it has a good return of investment because we have to maintain less code use, a smaller number of libraries and stuff like that, which greatly increases the cost of our software development.

What it saves is that when a developer writes something, he can feel free to post it for review, then release it. We are sure that if something comes up, then it will be raised by the automated tool and we will be ready to assess and resolve it. We are saving time on extensive code reviews that were happening in the past..”

**Aggelos Karonis**

Technical Information Security Team Lead at Kaizen Gaming

[Read full review](#) 

# Use Case

“The product scans runtime and that is our main use case. We have deployed it for one application in our testing environment, and for the other one on in our Dev environment. Whatever routes are exercised with those environments are being scanned by Contrast..”

## Verified user

Product Security Engineer at a tech services company with 10,001+ employees

[Read full review](#) 

“Up to this point, as an information security company, we had very limited visibility over the testing of the code. We have 25 Scrum teams working but we were only included in very specific projects where information security feedback was required and mandatory to be there. With the use of Contrast, including the evaluation we did, and the applications we have included in the system, we now have clear visibility of the code..”

## Aggelos Karonis

Technical Information Security Team Lead at Kaizen Gaming

[Read full review](#) 

“We've been using Contrast Security Assess for our applications that are under more of an Agile development methodology, those that need to deliver on faster timelines.

The solution itself is inherently a cloud-based solution. The TeamServer aspect, the consolidated portal, is hosted by the vendor and we have the actual Assess agent deployed in our own application environments on-prem..”

**Verified user**

Manager at a consultancy with 10,001+ employees

[Read full review](#) 

---

“Contrast Security Assess has a really good UI and gives the details in more depth. It gives more information about web application vulnerabilities. If third-party libraries, JS files, and JAR files have any CVEs in them, the solution reports that and gives a grade from A to E. It gives good information about vulnerabilities. It does the secure source code review, and the vulnerability it reports gives the file name and the line numbers indicating the issue and where it is..”

**Mustufa Bhavnagarwala**

CyberRisk Solution Advisor at a consultancy with 10,001+ employees

[Read full review](#) 

“The primary use case is application security testing, where we try to identify vulnerabilities within applications developed by our company.

Contrast a cloud-hosted solution. That's where most of the data and analysis takes place. It's also how most users interact with that data. Data is collected by agents that are deployed to servers within our environment. The agent component is internal to our organization, gathering data that is sent back to the cloud..”

**Verified user**

[Read full review](#) 

Director of Threat and Vulnerability Management at a consultancy with 10,001+ employees

---

“A good use case is a development team with an established DevOps process. The Assess product natively integrates into developer workflows to deliver immediate results. Highly accurate vulnerability findings are available at the same time as functional /regression testing results. There is no wait for time-consuming static scans.

Assess works with several languages, including Java and .NET, which are common in enterprise environments, as well as Node.JS, Ruby and Python. .”

**Verified user**

[Read full review](#) 

Senior Customer Success Manager at a tech company with 201-500 employees


# 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.

“I have no direct experience with the initial setup, but I needed a couple of proofs of concept for comparing Contrast with one of its Spanish competitors. .”

**Paolo Da Ros**

Founder at a tech services company with self employed

[Read full review](#) 

“The product's setup is easy. I would rate it a ten out of ten. The tool's deployment took one day to complete. The engineers from Contrast did an analysis and submitted a report post which we initiated the tool's installation. .”

**AggelosKaronis**

Senior Manager of Information Security at Kaizen Gaming

[Read full review](#) 

“Assess is easy to deploy and has the same learning curve as Protect. You must be familiar with your JVM to add the agents. Other than that, it's pretty straightforward. I set it up with two different people. .”

**ToddMcAlister**

[Read full review](#) 

Lead Application and Data Security Engineer at a insurance company with 5,001-10,000 employees

---

The agent installation is straightforward. Typically, for an initial user (developer) and application, Customer Success or Professional Services can just walk them through the setup over the phone. The dashboard requires no installation (SaaS), so the developer can exercise the app + agent and see vulnerabilities immediately.

Some deployments are more complex, but deployment complexity generally reflects the complexity of the customer and their overall situation. A large customer may have many business units, app teams, apps, and languages, requiring some planning.

**Verified user**

[Read full review](#) 

Senior Customer Success Manager at a tech company with 201-500 employees

---



“The setup is very straightforward. Something that has worked greatly in their favor: The documentation, although extensive, was not very time consuming for us to prepare. We have a great team and had a very easy integration. The only problems that we stumbled onto was when we didn't know which solution would work better for our production. Once we found that out, everything went very smoothly and the operation was a success.

The final deployment: Once the solution was complete, it took us about less than a day. However, in order to decide which solution we would go with, we had a discussion that lasted two or three working days but was split up over a week or so to have the feedback from all the teams. The deployment was very fast. It took one day tops..”

**Aggelos Karonis**

Technical Information Security Team Lead at Kaizen Gaming

[Read full review](#) 

“The initial setup was both straightforward and complex. Getting the agent deployed to environments can be complex when people don't understand how it works. But once that agent is deployed, it's very simple. The agent starts gathering data immediately and the data is presented in a UI in a way that is easily understood. You pretty much have vulnerability data right away. The only hurdle is making sure that you've got the agent deployed correctly. After that, everything is very simple.

Deployment for us is ongoing, as we continue to add applications. If I were to just choose one application and look at how long it takes to deploy to that environment, if the application owner has the resources and the ability to deploy the agent, it could be done in a few hours.

In our case, because deploying the agent is a change to the environment, sometimes that impacts larger processes like change management or making sure that the appropriate resources are assigned to do that work. If you have a large environment with many servers that need to have the agent deployed, it could take days or weeks if you don't have the resources to do it. That's not really a weakness of Contrast, but I think it's important to be aware of that if an organization is going to deploy this. A security team like mine might have external dependencies. When it comes to a legacy scan, we might not need anybody's input for us to run it. But with Contrast, we definitely need other teams to help us deploy the agents. Those teams include application owners, cloud services, server management. Whoever is responsible for installing software on a server in your environment would have to participate in this process. It's not something that the security team can do alone.

A good implementation strategy would be

- having an application inventory
- knowing where you're going to deploy this
- ensuring that your applications are using technologies that are supported by Contrast.

One of the things that we've done internally to try to simplify the agent deployment process is that we give the development teams a package that includes

the agent, instructions for deploying the agent, and a couple of other properties that are included in the agent to help us with overall organization. At that point, it really is just a matter of getting the agents installed.

Once you're gathering data, you want to work with development teams to make sure that they have access to the data. Once you're gathering data, that's when you can start working with integration points, because Contrast does allow you to create tickets in bug-tracking systems or to send alerts to communications platforms. Gathering the data is just the beginning of the process. There's also the dissemination of that data. That part is really dependent on how your organization utilizes and communicates vulnerability data.

We have under 50 users of the solution and about 80 percent are developers, while 10 percent are program management and the other 10 percent are in security. Aside from security, they're all consumers of data. The security users operate the platform, make sure that everything is in order, that applications are being added correctly, and that integration is being added correctly. All of the other users are people who are logging in to view vulnerabilities or to review the state of their applications or to gather reporting data for some deliverable. They don't actually operate or manage the platform. I'm the primary operator.

In the security department, our role in deployment and maintenance is creating those packages that I referred to earlier, packages that tell the developers or the application owners how to deploy the agents. It's the application owners who are responsible for a lot of the maintenance. They're the ones that have to make sure that the agent is part of their build process, they have to make sure that the agent is reporting correctly, and they have to make sure the agent is deployed to servers that are associated with their application. It's the agent that feeds the platform, so a lot of the maintenance is associated with maintaining the agent..”

**Verified user**[Read full review](#) 

Director of Threat and Vulnerability Management at a consultancy with 10,001+ employees

# Customer Service and Support

“I don't think I've ever called their tech support. I've always either opened tickets through the web UI or by email. Overall, my experience with them is positive. I can't think of an occasion when they've failed to either provide me resolution or understand my issue well enough to have it escalated to other product teams that were able to resolve my issues..”

## Verified user

[Read full review](#) 

Director of Threat and Vulnerability Management at a consultancy with 10,001+ employees

---

“Many tickets have been raised to understand some functionality or issues in what the solution reports. We can customize the issues that Contrast Security Assess gives. A ticket was raised to the support team for the customization we wanted. They took some time to understand the customization we actually wanted. It would have been better if their response was more quick..”

## Mustufa Bhavnagarwala

[Read full review](#) 

CyberRisk Solution Advisor at a consultancy with 10,001+ employees

---

“On a scale from one to five, Contrast technical support is about a four. I haven't had too many support issues just yet, but in each one that I have had, they have been very quick to respond; within hours as opposed to days. I haven't rated it a five just because I haven't had enough support requests to see if they are any different than other software vendors out there..”

**Verified user**

[Read full review](#) 

Manager at a consultancy with 10,001+ employees

---

“They have a cool, amazing support team that really helps us. I've seen a bunch of other vendors where you put in tickets and they get back to you after a few days. But Contrast responds really fast. From the word "go," Contrast support has been really awesome.

That's their standard support. They don't have premium support. I've worked with different vendors, doing evaluations, and Contrast is top-of-the line there..”

**Ramesh Raja**

[Read full review](#) 

Senior Security Architect at a tech services company with 5,001-10,000 employees

---

“Their level of support and troubleshooting for the product is limited because of how they handle troubleshooting. It's done through a log file that's very cumbersome to work with.

Their technical support staff is very responsive. Personally, I've put in about 60 support tickets with Contrast. Some of the support tickets have ended up being actual changes to the product itself. Overall, I'm pretty pleased with that. But they're definitely still growing. They're a small company that is on the verge of growing into a very big company. I can tell from the quality of support I'm getting that they're struggling to keep up with that demand..”

**Verified user**

[Read full review](#) 

Director of Innovation at a tech services company with 1-10 employees


---

“Every time that we approach them with a request, we have had an immediate response, including the solution, with the exact point in the documentation. Therefore, they have been very helpful.

It was a very smooth completion of the paperwork with the sales team. That's a positive as well because we are always scared by the contract, but they monitor it on a very efficient level.

I really want to highlight how enthusiastic everyone is in Contrast, from day one of the evaluation up until the release. If we think that we should change something and improve upon it, then they have been open to listening and helping. That is something that greatly suits our mentality as an organization. .”

**Aggelos Karonis**

[Read full review](#) 

Technical Information Security Team Lead at Kaizen Gaming

## Other Advice

“Contrast Security Assess is deployed on-cloud in our organization.

I would recommend Contrast Security Assess to other users. It's a really good tool. It provides lots of details on web-based vulnerabilities, source code reviews, and third-party library issues.

Overall, I rate Contrast Security Assess an eight out of ten..”

**Mustufa Bhavnagarwala**

CyberRisk Solution Advisor at a consultancy with 10,001+ employees

[Read full review](#) 

---

“Start with a small app team initially, before scheduling a larger rollout. Teams that have been using SAST tools find that using Assess changes how they think about appSec in their development workflow and helps them identify process modifications that maximize the value of the tool.

Overall, on a scale from one to ten, I would give this solution a rating of ten. The product is strong and improving, support is responsive and effective, and supported integrations work for many customers. .”

**Verified user**

Senior Customer Success Manager at a tech company with 201-500 employees

[Read full review](#) 

---

“Make sure you understand your environment before deploying. Try to get an idea of what technologies are in use by applications so you can group them and group

the deployment and the implementation. That way you can focus on automating .NET deployments, for example, first, and then move on to Java, etc.

The biggest lesson I have learned from using this solution is that there is a tool out there that is really changing the way that we are running security testing. In the security realm we're used to the static and dynamic testing approaches. Contrast Assess, as well as some other tools out there, has this new feature of interactive application security testing that really is the future for developer-driven security, rather than injecting security auditors as bottlenecks into the software development life cycle.

I would rate Contrast Security at eight out of 10, and that is because of that the lack of client-side support and the troubles in automating the deployment holistically across an organization..”

---

**Verified user**

Manager at a consultancy with 10,001+ employees

[Read full review](#) 

“I would recommend trying and buying it. This solution is something that everyone should try in order to enhance their security. It's a very easy, fast way to improve your code security and health.

We do not use the solution's OSS feature (through which you can look at third-party open-source software libraries) yet. We have not discussed that with our solutions architect, but it's something that we may use in the future when we have more applications onboard. At this point, we have a very specific path in order to raise the volume of those critical apps, then we will proceed to more features.

During the renewal, or maybe even earlier than that, we will go with more apps, not just three.



One of the key takeaways is that in order to have a secure application, you cannot rely on just the pentest, vulnerability assessments, and the periodicity of the reviews. You need the real-time feedback on that, and Contrast Assess offers that.

We were amazed to see how much easier it is to be PCI-compliant once you have the correct solution applied to it. We were humbled to see that we have vulnerabilities which were so easy to fix, but we wouldn't have noticed them if we didn't have this tool in place.

It is a great product. I would rate it a nine out of 10. .”

**Aggelos Karonis**

Technical Information Security Team Lead at Kaizen Gaming

[Read full review](#) 

---

“The IAST adoption in Italy, at least, is slow. My customers' feedback is that their commercial aptitude could be more flexible. It needs to be more flexible. They need to understand that they have an opportunity window that will last only a few years. And they are selling to win market share now, wherein in the next two years, everybody will be doing IAST. Whether it is good or bad, more or less, everybody will be doing that because the proposition is unbeatable.

I recommend others to try the solution because it is the most rewarding investment you can make in security access, apart from end-user training and user-awareness training.

But my bad side is that I think three, four years in advance. For example, I made a marketing campaign on VPNs in nineteen ninety-eight. Because VPNs were unbeatable, and it took another ten years before the market took off.

So I'm sure it will happen. Especially in the Italian market, there are market specifics because, in Italy, most of the development is outsourced, and very little

development is done in-house.

So the big customers usually do not make the investment. The company which generates the code should be tailored to be bought by the leading company, which then uses the product to assess the work. Technology vendors usually focus on technology, and companies focus on organizational processes. So I was trying to sell outlets, which now are IBM source good edition, Upscaler. I was selling outlets to telecoms and proposing ounce levels as portfolio management. So that they have thousands of applications and you have a tool that assesses any given application's security. And the problem was that the guys in charge of the portfolio were not supposed to have access to the code.

So there was an additional problem stopping the customer from buying a perfect technological solution. They could manage the security, but the guys managing the application portfolio were not supposed to add access to the source code. And so they were not the proper organization for the thing to happen. And this is a problem which in large customers is quite frequent. But, again, you should see any market, a single customer, the needs, the processes, the power struggle, and data on a power struggle; it's more complicated though it can be done.


I would give Synopsys a nine because no one is at ten today.

I have ranked Contrast just below Synopsys because Synopsys has the size and the scope, and they have an internal vertically integrated solution apart from all the partnerships you could have. Since Contrast is a much smaller company, they should enter into some partnerships.

I rate the overall solution an eight out of ten..”

**Paolo Da Ros**

Founder at a tech services company with self employed

[Read full review](#) 

“Be prepared for the cultural change, more than the technology change. Most of the benefits that I have from the solution are the time savings where we're not scanning things and analyzing things. I now spend a lot of my time explaining to people how Contrast works, explaining to people how it changes our program, and explaining to people how Contrast fits into their development life cycle. If you're approaching it from a purely technical perspective, you're missing a big piece of what you're going to be spending your time on.

I don't have any major complaints. Most of our challenges with Contrast have been how it changes our program and how it impacts the internal culture around development. Those are not really issues with the product itself. If we have had any kind of technical hurdle, it would be that a lot of our application owners might not understand the process for deploying the agent, which is when they instrument their environment. So we spend quite a bit of time supporting that part of the process, technically, which is not necessarily a good fit for a security program, having to tell people how to install an agent.

It gathers data in real time, it gathers data from agents. It doesn't perform scans, rather, it observes traffic, and that's fundamentally different from the other tools and from how those tools are used in our existing processes. We spend a lot of time on culture and process and explaining how the technology is different.

I find it very intuitive, but our users do not. We have developers who have spent the past 20 years thinking of application security in terms of a scan, and they're passive in that activity. The scan is something that's done for them, it's done to their environment, and then they're given data. Contrast is passive, it's an agent that's just gathering information, but it gives it to them directly, and that means they have to participate. They have to ingest that information, they have to be prepared for what they're going to do with it. They're not used to having that role. They're used to being the recipients of information or they're used to other people performing the service of scanning their environment, and Contrast doesn't do that.

The biggest lesson I've learned is around how our developers think about security. When they're passive in that process, when somebody else is running scans for

them and telling them what to fix, the way that they operate is different than when you give them an agent in their environment and you start giving them data from multiple environments and you start automatically sending that information to a bug tracker that they use. It's the automation and visibility that they've been asking for. But now that they're getting it, they are not exactly sure what to do with it.

I was not prepared for having to have conversations about culture and process. Now that I have a better understanding of how our developers operate, what their metrics are, and how they're evaluated, as well as what constitutes success and what constitutes security on their part, it gives me a much better idea of how to interact with them. Before, we would talk about how we're seeing a certain type of security issue in our environment, and then we would try to figure out why our developers were continuing to make that mistake. Now, it's more about how developers utilize security data in their process and how we can improve that.

Right now, the visibility the solution gives us is probably a little bit painful, because this is data that the developers didn't have before. We're identifying more vulnerabilities, and that is something they were not expecting. They were used to results that originated from our previous tools and they only had a handful of vulnerabilities to address. Contrast is now finding more issues with their applications as well as finding issues that are associated with libraries. That's a lot more data than they're used to receiving. And potentially, they're surprised by how vulnerable their applications are.

The initial impact of having additional vulnerabilities that you were previously unaware of seems like a significant resource impact. A developer who normally only had to deal with a handful of findings may now have 10 or 20 or 100 findings to deal with. That may feel like a resource burden because you now have more things to fix, but ultimately that's going to be less expensive than the cost of a breach or loss of contract or anything else that might affect the business in the larger sense..”

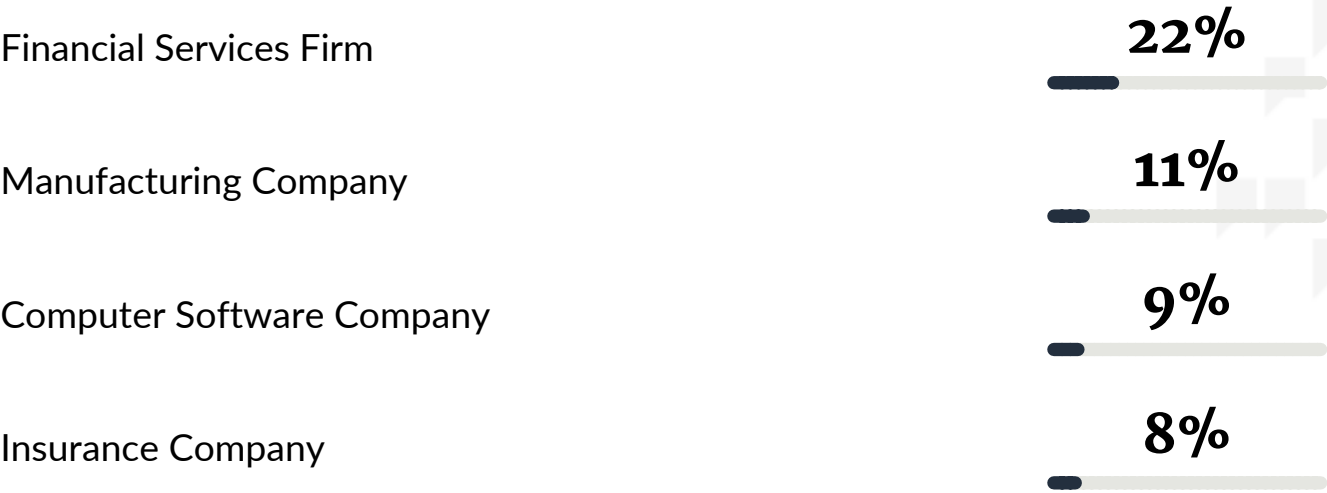
**Verified user**

Director of Threat and Vulnerability Management at a consultancy with 10,001+ employees

[Read full review](#) 

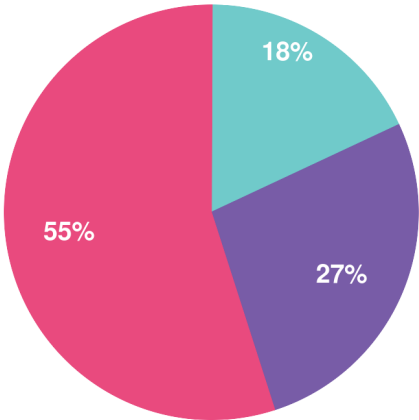
# Top Industries

by visitors reading reviews

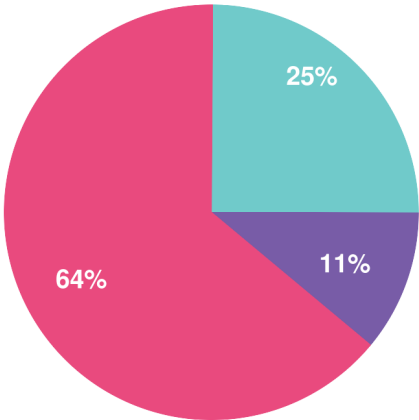


# Company Size

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](http://www.peerspot.com)

## PeerSpot

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

[reports@peerspot.com](mailto:reports@peerspot.com)

+1 646.328.1944