aws marketplace

Acunetix

Reviews, tips, and advice from real users






Powered by PeerSpot

Contents

Product Recap

Acunetix

Acunetix Recap

Acunetix is a dynamic application security tool used globally for web application vulnerability scanning, focusing on SQL injection and cross-site scripting.

Acunetix provides a comprehensive web vulnerability assessment platform designed for identifying and remediating security threats. Users benefit from its ability to schedule scans, boasting a fast detection rate for common vulnerabilities. The tool's centralized dashboard helps organizations with compliance monitoring and features such as crawling and login sequence enhancements, contributing depth to its security assessments. Despite high praise for its integration capabilities and automated scanning that saves time, pricing and false positives present challenges. Organizations often use Acunetix to maintain internal security and evaluate pre-release environments.

What are Acunetix's main features?

- Comprehensive Reporting: Detailed reports assist in security analysis and compliance audits.
- User-Friendly Interface: Simple navigation enhances user experience.
- Scheduled Scans: Automation of scans allows for continuous monitoring.
- Fast Detection: Quickly identifies vulnerabilities like SQL injection and cross-site scripting.
- Integration Capabilities: Scalable solutions with compatibility across applications.
- Crawling & Login Sequence: Improves depth in security analysis.

What benefits should businesses look for in reviews?

- Low False Positive Rate: Accurate vulnerability detection saves time in analysis.
- Time Efficiency: Automated scans reduce manual workload, improving team productivity.
- Scalability: Integration features help accommodate growth and complexity.
- Compliance Support: Centralized dashboard supports regulatory compliance checks.

In industries like finance, healthcare, and technology, Acunetix assists in protecting sensitive data through robust scanning and reporting capabilities. Its ability to perform dynamic assessments makes it a chosen tool in regulatory environments and development settings, offering both internal security inspections and pre-release evaluations.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- "Acunetix helps reduce the man-days and effort needed for scanning bulk applications through automated assessments, allowing good dashboard visualization that can be reported easily to management, providing complete visibility on vulnerability metrics."

Rahul Kumar

Senior Engineer - Penetration Tester at a government with 10,001+ employees

- "If an organization has 100 plus applications and wants to use an automated scanner, they should definitely go ahead with Acunetix because it is very cost-effective and will save time compared to focusing on other solutions and performing manual security assessments."

Himanshu_Tyagi

Lead Cybersecurity at TBO

- "I appreciate the features that Acunetix has for the speed and the fact that it is in the cloud, which does not put any resources in my network, so I can set up a scan, go to bed, come back, and see the reports in my email."

Adetunji Adeoje

Team Lead, Application Security at a financial services firm with 5,001-10,000 employees

"The solution is excellent at detecting SQL injection and cross-site scripting vulnerabilities."

KashifJamil

CEO at Xcelliti

"I find it to be one of the most comprehensive tools, with support for manual intervention."

Abdullah Ozkan

Information Security Engineer at Tübitak Bilgem

"The product is really easy to use."

Kamil Matusik

Head of Operations, Supply Chain at Lyreco Deutschland GmbH

"The features of Acunetix have proved most effective in identifying vulnerabilities."

Srinivas Walikar

Senior Business Development Manager at Intouch World

What users had to say about valuable features:

"I mainly configure the tool for web applications, and I evaluate all products on the market. I find it to be one of the most comprehensive tools, with support for manual intervention. It offers support for specific scenarios like CAPTCHA and supports the ability to manage actions and updates from the internet.."

Abdullah Ozkan
Information Security Engineer at Tübitak Bilgem

Read full review

The features of Acunetix have proved most effective in identifying vulnerabilities. I find the false positives to be a notable aspect. Additionally, with its impressive capabilities, Acunetix offers several options for deployment. I can use it both on the cloud and on-premises, which provides flexibility. Its most valuable role is in enhancing security by identifying potential vulnerabilities efficiently.

Srinivas Walikar
Senior Business Development Manager at Intouch World

Read full review

"I appreciate the upload function in Acunetix that allows me to upload so many targets at the same time in a CSV file. I also love the comprehensive reports that can generate a single report to capture all my scans, irrespective of the numbers. I appreciate the scheduling feature; when I want to schedule my scan, maybe weekly or quarterly, it scans and produces a report for me and sends it to my email. On the latest platform, Invicti, I appreciate the speed, which is quite fast, and the interface is also great.

The continuous scanning feature in Acunetix is one of the features I appreciate most because I can use it to schedule my scans and be notified if there are any changes. I can do comparative scans to know if I scan this Monday and send a report to my engineer, and they can do remediation. I can do comparison to know the aging of any vulnerability that has existed for a period of time. I can track what they have closed and what they have not closed within the relevant application scope.."

Adetunji Adeoje

Team Lead, Application Security at a financial services firm with 5,001-10,000 employees

Read full review

"The crawling option in Acunetix is really good because whenever a scan is initiated, the crawling option provides good coverage about the vulnerabilities identified in the application. The attack option that comes after crawling is quite good. When the application is configured in authenticated scan mode with Acunetix, it provides good visibility about the security vulnerabilities in the application.

"The experience with Qualys Total Cloud was really good, as when Qualys Guard was used to scan cloud security assets, it identified the vulnerabilities and helped differentiate between valid findings and invalid findings. Qualys Guard is called Total Cloud, which means cloud assets are scanned regardless of any environment, whether it is GCP, AWS, or Azure.."

Himanshu_Tyagi
Lead Cybersecurity at TBO

Read full review

“Acunetix has a very good ratio of fewer false positives, so users don't need to retest everything.

“Acunetix operates smoothly with no interruptions required, and it performs at 100% efficiency without issues in scanning anything.

“The solution is excellent at detecting SQL injection and cross-site scripting vulnerabilities.

“Acunetix integrates with every type of tool, including CI/CD tools, offering 100% integration in DevOps environments.

“The main benefit of Acunetix is that at the first level, users can address security issues related to penetration testing, allowing them to expose vulnerabilities and ensure all required testing is completed with very few false positives..”

KashifJamil
CEO at Xcelliti

Read full review

"The best feature Acunetix offers is the centralized dashboard and the quality of reports it generates, which includes various options for selecting reports and developer options for directly sharing the reports with developers.

"The centralized dashboard of Acunetix gives visibility into the security aspects of mass applications; for instance, with more than 200 applications, it provides a valuable overview of findings and necessary fixes, along with a high-level summary that helps us achieve compliance through monthly and sometimes weekly scanning.

"In terms of reporting, Acunetix is excellent because it can generate different types of reports, such as an executive summary report, detailed reports, and developer reports that can be shared directly with developers.

"Acunetix positively impacts my organization by helping identify outdated libraries and applications, including legacy applications vulnerable to old attacks based on OWASP Top 10, thus aiding in compliance checks for PCI DSS and OWASP.

"Acunetix provides a centralized report with compliance-related aspects and a vulnerability timeline, effectively helping reduce vulnerabilities and save time.."

Rahul Kumar

Senior Engineer - Penetration Tester at a government with 10,001+ employees

Read full review

Other Solutions Considered

"I have used Snyk, Qualys, and Tenable. I have worked with other tools that are more helpful and have more functionality than Acunetix. Acunetix is suitable for small companies.."

Kamil Matusik
Head of Operations, Supply Chain at Lyreco Deutschland GmbH

Read full review

"Although we are working with Acunetix, we are planning to migrate to Nessus in the future. We used Nessus around seven or so years ago. The current solution is a good one, however, my organization wants to try a new, different product. That is the reason we now moving to Nessus.."

Anubhav Goswami
Security Specialist at a tech services company with 11-50 employees

Read full review

"Acunetix is the fastest scanner available compared to applications like Netsparker and Fortify WebInspect. The longest scan with Acunetix, and it was for a huge web application, took only four hours. Other scanners did the job in six to eight hours.

While I like Netsparker, it is really slow compared to other scanners.."

Verified user
Security Engineer at Secure Network

Read full review

"I use Acunetix and Burp Suite together and they are both quite good. I use them to validate one another. If I want to compare Acunetix, I could also compare it with some other penetration test assessment tools, such as the one by Invicti, Netsparker, which I used to love, but I do not know if it is still around.."

Adetunji Adeoje
Team Lead, Application Security at a financial services firm with 5,001-10,000 employees

Read full review

"Acunetix stands out with its metrics, features, and Proof of Exploit. Other solutions we've used don't have those.

There is also Tenable.io Web App Scanning. Tenable's advantage is how it handles vulnerability management. For example, if you have Ansible vulnerability management, you can see both sets of information in a single pane. The only other difference might be pricing, but I'm not entirely sure about that.."

JanetMuhia
Cyber Security Engineer at Spartec

Read full review

"As far as experience is concerned, only Checkmarx SAST tool has been worked on, and no other Checkmarx products like Checkmarx One are used.

"Rapid7 Nexpose has been used, but no other Rapid7 products have been explored. Additionally, Qualys Guard and Qualys VMDR Vulnerability Management Detection Response solution have been worked on.."

Himanshu_Tyagi
Lead Cybersecurity at TBO

Read full review

ROI

Real user quotes about their ROI:

"I have seen a return on investment, as Acunetix helps reduce the man-days and effort needed for scanning bulk applications through automated assessments, allowing good dashboard visualization that can be reported easily to management, providing complete visibility on vulnerability metrics.."

Rahul Kumar
Senior Engineer - Penetration Tester at a government with 10,001+ employees

Read full review

"We have seen ROI with Acunetix. That's the most convincing point I have to prove to my management when it comes to the next budgeting cycle. The ROI is seen in the fact that, at the time of application releases, we hold off the risk. When we do the assessment, we see that the distributed cost of Acunetix, across all our releases reduces our risk. It's a very convincing point.."

Saminda Jayawardene
Compliance Manager at a tech services company with 201-500 employees

Read full review

“It saved us many weeks of work.

We didn't sell anything with Acunetix, so it was just an improvement for ourselves.

If someone would have hacked us, they probably would have caused much damage. However, now with Acunetix, they shouldn't be able to cause to damage..”

Verified user
Security Engineer at Secure Network

Read full review

“We found it to improve our processes and findings.

The solution is paying for itself, as our applications are more secure.

We have found several hundred medium to high level vulnerabilities in our applications. In just one application, we were able to identify 75 of these vulnerabilities..”

Verified user
Senior Security Engineer at a insurance company with 10,001+ employees

Read full review

“I can't share data points, but we have seen ROI. Otherwise, we wouldn't have renewed the license. Every year we evaluate if we're going to keep a vendor or not. Since we have renewed our license, we think it has ROI value.

It's impossible to answer whether it has saved us money in the long-term, but of course, since we use automatic tools, we don't need as many personal testers. However, personal testers also find a lot of bugs that automatic tools don't find. You need a combination of both..”

Verified user

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

Read full review

“Return on investment is hard to track because it really depends on the criticality of the vulnerabilities and what the business costs or impact could be if those vulnerabilities were actually exploited. We have a vigorous application security program so testing activities like SAST and DAST must take place. I know if we were to remove our DAST program and not test our websites, we could see an immediate cost-effect as a result. But since Acunetix is used as a secondary tool, we don't know if it actually provided any real cost metrics where we could say: "Okay, because of our use, we have saved X amount of dollars because it found Y amount of vulnerabilities that saved us Z amount of time remediating." Those metrics are not known..”

Verified user

Senior Security Engineer at a media company with 1,001-5,000 employees

Read full review

Use Case

“We needed it to scan our internal network and web applications.

Our security team of five people used it. We scheduled some monthly scans for web applications, which were not being used, to check for vulnerabilities and also vulnerabilities on new features..”

Verified user
Security Engineer at Secure Network

Read full review

“My main use of Acunetix is to scan my web application. I mostly deal with web applications and with Acunetix Network Security Component, but I have not activated the network component before and will not use it..”

Adetunji Adeoje
Team Lead, Application Security at a financial services firm with 5,001-10,000 employees

Read full review

"It is top-rated and widely employed for conducting security assessments on networks, websites, and applications. It is considered the gold standard for evaluating security measures and identifying vulnerabilities in websites, networks, and applications. The tool's extensive capabilities make it a go-to choice for ensuring security. It is renowned for its comprehensive scanning and assessment of networks and websites, but it is also known for its significant cost, particularly for deploying it on large clusters.."

Jagobandhu Some
Hardware Engineer at Ministry of Defense

Read full review

"Most of the customers who use Acunetix are looking for security testing. The primary use case is performing penetration testing.

"The main use cases include vulnerability scanning, security testing, penetration testing, PCI DSS reporting, and multi-user environment support, which excels in SQL injection and cross-site scripting detection.."

KashifJamil
CEO at Xcelliti

Read full review

"Acunetix has primarily been used for application security, and it has also been used for vulnerability management, though not as extensively because Qualys Guard Total Cloud solution was being used for scanning cloud assets.

"Qualys Total Cloud was used to scan cloud assets. Earlier, when using CLI tools like Troller, there was not much visibility because the reporting section from the CLI tool was not that helpful. However, when using Qualys Guard, the Total Cloud offered advanced reporting features and had the option to share vulnerability reports directly via email, allowing the end participant's email address to be entered for automatic report delivery.."

Himanshu_Tyagi
Lead Cybersecurity at TBO

Read full review

"I have been using Acunetix for more than five years, as I used it in both my previous company and my current company.

"My day-to-day use of Acunetix involves scanning web applications, scanning multiple files, and conducting gray-box scanning of the applications to identify any automated issues related to outdated libraries.

"I rely primarily on Acunetix for bulk scanning of multiple web applications, which includes gray-box and white-box assessments as well as black-box assessments of web applications in terms of security.

"One specific example of a recent assessment I did with Acunetix involved a large customer-facing application with many modules and functionalities that cannot be done manually, so it was very efficient; we included active scanning of Acunetix through gray-box credentials and identified a few vulnerabilities that were not found manually.."

Rahul Kumar

Senior Engineer - Penetration Tester at a government with 10,001+ 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.

"Acunetix is easy to install and took only two minutes to deploy. For desktop applications, you need to download an EXE file. Deployment over the cloud requires API. ."

Amr Abdelnaser

Senior Information Security Analyst at EastNets Holding Ltd.

Read full review

"The setup process for Acunetix is not that complicated, and Acunetix support can always be reached out to. Whenever Acunetix is onboarded in the environment, the Acunetix team assists with the installation, making the setup quite easy.."

Himanshu_Tyagi

Lead Cybersecurity at TBO

Read full review

"The initial setup was easy because we had a proper software team consisting of developers, database administrators, and application teams. With the help of the vendor, we were able to implement it successfully. It took approximately three to four months.."

AnubhavGoswami

Read full review

Compliance Manager at a recruiting/HR firm with 1,001-5,000 employees

"For standard use cases, we deploy it on a notebook or a desktop machine. In case of integration with a development system, we deploy it on a server or a virtual memory machine. I rate the solution's initial setup process a five out of ten.."

Michael Poon

Read full review

Director at NETdefence Co. Limited

"It is a bit complicated, but their support is very good in case of any issues. It can be on-prem or on the cloud. It depends on what the customer wants.

You don't need more than one person for its maintenance.."

MarceloPrintac

Read full review

VP Business Development at MultiPoint Ltd.

"I work with on-premise and on-the-cloud products. I faced a huge problem when I tried to install cloud agents. We needed a proxy connection, but Acunetix had a problem creating the connection. I worked with the support for a month. It started working, but the agent caused the bug.."

Kamil Matusik

Head of Operations, Supply Chain at Lyreco Deutschland GmbH

Read full review

Customer Service and Support

"I would rate technical support from the vendor as very good. Their customer support representative supports very well. Once I send an email, they respond quickly and without delay, so I would say they are quite supportive.."

Adetunji Adeoje
Team Lead, Application Security at a financial services firm with 5,001-10,000 employees

Read full review

"Acunetix customer support responds on time, but resolution can take longer due to involving stakeholders who are not relevant and the support staff not being familiar with the problem.."

Rahul Kumar
Senior Engineer - Penetration Tester at a government with 10,001+ employees

Read full review

"I have requested support from the vendor regarding our scan results that have false positives. The vendor double checks and adds a patch if needed. However, their response is too slow.."

Le Viet
Security Consultant at VNCS

Read full review

"The Acunetix team is in Malta. They are very good, and they provide support over the phone. They are available 24 hours a day, and they answer your queries very fast. They're very active and good.."

MarceloPrintac
VP Business Development at MultiPoint Ltd.

Read full review

"I am not very satisfied with the customer support they provide. It tends to be quite time-consuming. When I raised a ticket seeking assistance with a simple issue, their response time was notably delayed. They mentioned having a backlog of inquiries, and it took a while for them to address my specific question. There seems to be a disconnect between the amount of money they charge for their support services and the level of support they provide.."

Jagobandhu Some
Hardware Engineer at Ministry of Defense

Read full review

"The tech support from Invicti for Acunetix is really good. Whenever a support ticket is raised, their SLA is quite nice. For high-severity issues, they reach out within two to three hours, and for critical issues, a response is received within 15 minutes.

"The tech support would be rated an eight out of ten.."

Himanshu_Tyagi
Lead Cybersecurity at TBO

Read full review

Other Advice

“I would generally recommend Acunetix to any organization in the IT-enabled sector. However, I have not worked for a non-IT organization, so I cannot comment on that.

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

AnubhavGoswami
Compliance Manager at a recruiting/HR firm with 1,001-5,000 employees

Read full review

“My advice for those looking into using Acunetix is to utilize it effectively due to its good features, especially its APIs and other functionalities. My company does not have a business relationship with this vendor beyond being a customer. I would rate this review as a seven out of ten..”

Rahul Kumar
Senior Engineer - Penetration Tester at a government with 10,001+ employees

Read full review

"We use Acunetix via API with our bucket. When developers try to push some part of the code, Acunetix is used to analyze the vulnerabilities. The integration of Acunetix with Jira and other buckets is easy. Acunetix is not very different from the other vulnerability scanners. It is not the best solution. The connection is via API. We get the link and change the token between the connections. The integration is not easy, but it's not hard. Bigger companies with a lot of developers can get better tools. Overall, I rate the tool a six or seven out of ten.."

Kamil Matusik
Head of Operations, Supply Chain at Lyreco Deutschland GmbH

Read full review

"Acunetix supports multi-user environments effectively.

"Acunetix is targeted for small to mid-size teams in a DevSecOps environment, making it the best choice for small and mid-size companies, offering a friendly interface, support for CI/CD, and excellent vulnerability scanning capabilities.

"On a scale of 1 to 10, I rate Acunetix 9 out of 10.."

KashifJamil
CEO at Xcelliti

Read full review

"I am still working with Acunetix, and we have even moved to their new platform, Invicti. I have requested a demo for Acunetix DeepScan technology, but I have yet to go through DeepScan. That was the next step we wanted to take right now. I have been speaking to the customer service team, and I would like to have a demo of Acunetix because right now we use Azure DevOps. I would have liked to see how it can be integrated with our Azure DevOps in the SaaS environment so it can be

used as a task from the CI/CD pipeline. I met Acunetix through a reseller at my current workplace, who provided the quotation. Overall, I would give Acunetix an eight out of ten.."

Adetunji Adeoje
Team Lead, Application Security at a financial services firm with 5,001-10,000 employees

Read full review

"Currently, work is being done with AWS cloud security and application security tools such as Burp Suite, and various automated scanners such as Netsparker and Acunetix are also being used, along with vulnerability scanning tools such as Nessus Professional and Rapid7 Nexpose.

"Acunetix is good, even though there have been some issues related to false positives. Whenever an automated scanner like Netsparker or Acunetix is used, it takes time to run the scan. Once the scan is completed, the false positives flagged by the scan need to be identified. Acunetix is a good tool because if there is less time and the team needs to perform the security assessment, a manual assessment will take almost a week to assess a large application. However, when an automated scanner like Acunetix is used, the same task can be done within three to four days. Authenticated scans are usually preferred with any automated scanner like Acunetix because it provides much visibility about the application on which the scan is initiated, and the results from authenticated scans are very good compared to unauthenticated scans.

"Acunetix was used recently, about three months ago.

"Acunetix was not used for AWS because various other AWS solutions are available to determine the vulnerabilities for cloud, primarily using AWS Inspector to scan the AWS cloud. Security Hub is also used to measure cloud security posture management, so when it comes to scanning the cloud, AWS Inspector is primarily used.

"Acunetix was hosted on the AWS cloud because when the application was

scanned, it was not an on-premises solution; the applications hosted in AWS cloud were scanned using Acunetix.

“The integration part has not been explored much because other tools are available, but Acunetix supports YAML files that can be used to integrate those scans into the CI/CD pipeline. However, Acunetix scans have not been integrated into the CI/CD pipeline.

“The Acunetix network security component has not been used.

“If there is less time to perform manual security assessments, Acunetix is a good option because if a manual security assessment takes almost a week, the same task with Acunetix can be completed within three to four days, which really saves time for the entire team. The results are faster and interactive reports generated by the dashboard can be shared. This helps improve the overall security posture.

“The features present in Acunetix are quite good and serve the purpose well.

“Acunetix is definitely recommended for scanning, and if someone asks whether they should use Acunetix to mitigate the threats identified in their applications hosted in AWS cloud, it would definitely be recommended.

“When the continuous scan approach is used for security compliance, it really helps because the scan is not paused for any reason, like if the application goes down. With the continuous scan operation, the application is continuously assessed by the scan engine of Acunetix, and the results from the continuous scan feature are quite good. The continuous scanning feature has been used.

“If an organization has 100 plus applications and wants to use an automated scanner, they should definitely go ahead with Acunetix because it is very cost-effective and will save time compared to focusing on other solutions and performing manual security assessments.

“The recommendation for other organizations considering Acunetix depends upon their requirements.

“This review has been given a rating of 7 out of 10..”

Himanshu_Tyagi
Lead Cybersecurity at TBO

Read full review

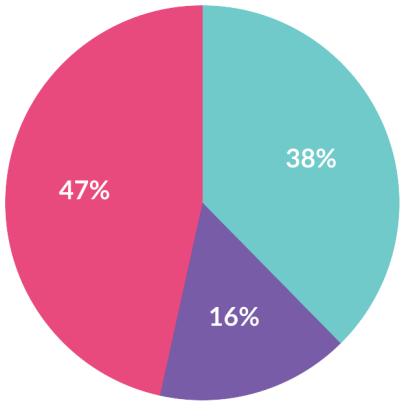
Top Industries

by visitors reading reviews

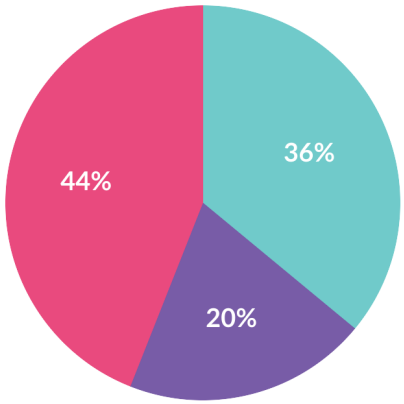
Manufacturing Company	12%
Financial Services Firm	11%
Computer Software Company	9%
Comms Service Provider	9%

Company Size

by reviewers



by visitors reading reviews



Large Enterprise Midsize Enterprise Small Business

About this buyer's guide

Thanks for downloading this PeerSpot report.

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

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

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

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

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

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

About PeerSpot

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

PeerSpot helps tech professionals by providing:

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

Use PeerSpot to:

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

Join PeerSpot to connect with peers to help you:

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

Visit PeerSpot: www.peerspot.com

PeerSpot

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

reports@peerspot.com

+1 646.328.1944