

aws marketplace

Aikido Security

Reviews, tips, and advice from real users



Powered by  PeerSpot



Contents

- Product Recap..... 3 - 4
- Valuable Features..... 5 - 12
- Other Solutions Considered..... 13 - 15
- ROI..... 16 - 18
- Use Case..... 19 - 23
- Setup..... 24 - 25
- Customer Service and Support..... 26 - 27
- Other Advice..... 28 - 31
- Trends..... 32 - 33
- About PeerSpot..... 34 - 35

Product Recap



Aikido Security

Aikido Security Recap

Aikido Security is the no-nonsense platform that empowers developers by centralizing code-to-cloud security issues and providing rapid guidance for fixing vulnerabilities.

With over 6,000 teams utilizing its features, Aikido Security prioritizes effective security management by consolidating 11 comprehensive scans into one platform. This approach translates complex vulnerabilities into understandable insights, targeting non-enterprise SaaS businesses with engineering teams of 10-500 developers. It focuses on delivering security management without excessive costs or complexity through a product-led growth model.

What are the standout features of Aikido Security?

- SAST: Secures code as it is written.
- DAST: Monitors surfaces, dynamically tests for vulnerabilities with OWASP ZAP.
- IaC: Detects infrastructure vulnerabilities.
- CSPM: Real-time detection of cloud infrastructure risks.
- Container Scanning: Assesses container environments for risky packages.
- Secrets Detection: Identifies exposed API keys, passwords.
- Open Source Dependencies: Analyzes dependencies to avoid vulnerabilities.
- Open Source License: Maps and exports SBOMs to manage license risks.
- Malware Detection: Protects from supply chain attacks.
- Runtime Protection: Secures apps with an embedded firewall.
- Custom Scans: Integrates with existing tools like SonarQube.

Why should you consider Aikido Security?

- Easy Adoption: Setup takes less than 3 minutes with clear UX.
- Cost Efficiency: Offers a comprehensive 9-in-1 solution at competitive pricing.
- Accurate Results: Best false positive reduction in the market.

In industries like software development and cloud services, Aikido Security is implemented to provide clear insights, enabling teams to focus on rapid product growth while maintaining robust security. Its product-led growth strategy, including a freemium offering, allows developers to experience benefits firsthand without initial investment.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- ✓ “Aikido Security nests directly in our development workflow and it catches security issues before they reach production.”



B Goswami

Product Manager at Zidio development

- ✓ “Aikido Security offers the best features including being very easy to use, allowing even a normal tech person with some hands-on experience to use this tool and clearly get the results they want.”



Aman Raj Pandey

Sr. Project Analyst [Cybersecurity] at a consultancy with 10,001+ employees

- ✓ “The biggest win with Aikido Security was reducing context switching, as developers previously received vulnerability reports from multiple tools and tried to figure out ownership manually, and now most findings are visible in one place.”



Imyashpatel Patel

Software Developer at Bisag-N

- ✔ “Aikido Security has positively impacted my organization significantly because initially we were thinking it would take a month for us to achieve SOC 2 compliance again, and with Aikido Security, we were able to get all codebase vulnerability fixes within a week for all our 13 or 14 repositories that we had.”



Samir Patil

Co-Founder & CTO at Mango Giraffe

- ✔ “Aikido Security saved me several hours each week by automating vulnerability scanning and security checks, reducing the need for manual review and helping me focus on more development.”



Abdulmunafz Mct

Full Stack Developer at Sri Krishna Arts and Science

- ✔ “Since switching to Aikido Security, I have noticed a positive impact on my team's productivity with measurable results, as we now have measurements.”



Francisco Javier Vergara

SecOps Engineer at IriusRisk

What users had to say about valuable features:

“Aikido Security offers vulnerability scanning, dependency monitoring, cloud security insights, cloud security checks, and an easy-to-use dashboard. The Aikido Security dashboard updates frequently, so I am able to access information in case of emergency or urgent situations. The dashboard itself is in a neat format and very clear-cut, so I am able to use it in an easy manner.

“It saves time by prioritizing importance and security issues and reducing alert failures. Aikido Security has improved my project security by helping me identify issues early and increasing my confidence before deployment. My favorite feature is the dependency vulnerability scanning because it quickly identifies the risk in third-party packages, which saves me time in finding vulnerabilities..”

Abdulmunafz Mct

Full Stack Developer at Sri Krishna Arts and Science

[Read full review](#) 

“The best features Aikido Security offers include instantly raising PR by just identifying the vulnerabilities.

When I say instant raising of PR, it helped my workflow by making the process super easy and quick. Initially, I thought I would need to pick the right vulnerability from the internet, update my codebase accordingly, and then ask an engineer to do it. This usually takes about three or four days for one vulnerability, and maybe a week for a bunch of vulnerabilities. However, with Aikido Security it took me two to three hours.

Aikido Security has positively impacted my organization significantly because initially we were thinking it would take a month for us to achieve SOC 2 compliance again. With Aikido Security, we were able to get all codebase vulnerability fixes within a week for all our 13 or 14 repositories that we had..”

Samir Patil

Co-Founder & CTO at Mango Giraffe

[Read full review](#) 

“Standout features of Aikido Security include secret detection, data-driven prioritization of findings, container scanning, and a consolidated security dashboard.

“The biggest win with Aikido Security was reducing context switching, as developers previously received vulnerability reports from multiple tools and tried to figure out ownership manually. Now most findings are visible in one place. For example, one issue went unnoticed for weeks, but we are now addressing it in active development, reducing the number of security issues discovered last minute in testing. The secret scanning feature caught a couple of accidentally committed credentials early on, such as an AWS API key committed to a repository, which would have eventually been found during a review, but catching it automatically was definitely a win. Additionally, onboarding new repositories is very straightforward compared to some enterprise security products that have been used..”

Imyashpatel Patel

Software Developer at Bisag-N

[Read full review](#) 

“Aikido Security offers the best features including being very easy to use, allowing even a normal tech person with some hands-on experience to use this tool and clearly get the results they want. If we go for DAST also, it is very good.

The ease of use of Aikido Security helps my daily workflow since I can upload my whole codebase, and it will identify at each line where the vulnerabilities are present and provide recommendations to fix and related vulnerabilities, detailing what those vulnerabilities are and how they will impact the whole code or the infrastructure.

Aikido Security has positively impacted my organization by reducing a lot of work to manually check each line of code; the process goes on and on. Iterations have increased due to manual work, but the iterations which earlier took around seven to eight are now only taking two to three. Using that, a lot of our time gets saved.

For a secure code review or SAST, usually we are taking around seven to ten days, but using Aikido Security, we complete the activity within two to three days..”

Aman Raj Pandey

[Read full review](#) 

Sr. Project Analyst [Cybersecurity] at a consultancy with 10,001+ employees

“In my experience, the best feature Aikido Security offers is its ease of use, as it was really easy to onboard our engineers into adopting Aikido Security in their day-to-day lives.

“The reason onboarding my engineers with Aikido Security was so easy is the user interface. The first thing our engineers see when they log in is a feed of vulnerabilities that their own repositories are affected by, which helps them focus only on their work at hand.

“I would also like to add that the integrations part is really useful, as all of the integrations we have added so far, mainly Jira, IDE, and API integrations, are really easy to use because they are backed by strong documentation that they maintain daily. This is a commendation to them.

“Aikido Security has positively impacted our organization by helping us reduce the complexity in managing our vulnerabilities. We now have a single source of truth with Aikido Security, allowing us to get rid of manually maintained automations that we previously had..”

Francisco Javier Vergara

SecOps Engineer at IriusRisk

[Read full review](#) 

“I used it mainly for three things. The first one is static code analysis, open-source dependency vulnerability scanning, and container image scanning. It has become our primary security layer in our development workflow.

“When talking about the features, there are several powerful features they have. The first one is static application security testing or SAST. It scans source code for vulnerabilities automatically.

“It identifies vulnerable open-source dependencies in our project. Container scanning checks Docker images for known vulnerabilities before deployment. Infrastructure as code scanning scans Terraform and other IaC files for misconfigurations.

“The unique feature is secret detection, which automatically finds accidentally committed API keys, passwords, or tokens in code. Also, Auto-Triage intelligently filters false positives so developers only see real, actionable issues.

“The impact was significant and immediate. Security shifted left, meaning issues were caught during development rather than after deployment. That alone reduced our remediation costs dramatically, since fixing issues early is always cheaper than fixing them in production. Developer confidence has increased. The team members felt more secure pushing code knowing Aikido Security was continuously scanning. Our comprehensive posture improved with clear visibility into all vulnerabilities across our entire codebase, which made security audits much smoother as well..”

B Goswami

Product Manager at Zidio development

[Read full review](#) 

Other Solutions Considered

“I haven't used a different solution, but I have listened about Checkmarx and other tools; however, they don't seem to perform well. I definitely used Aikido Security, and after that, I don't want to switch to any other. It is very good..”

Aman Raj Pandey

Sr. Project Analyst [Cybersecurity] at a consultancy with 10,001+ employees

[Read full review](#) 

“Before Aikido Security, I mainly relied on manual checks and basic security tools, which were less comprehensive. I was supporting multiple projects and repositories through manual methods and basic security tools that were less comprehensive..”

Abdulmunafz Mct

Full Stack Developer at Sri Krishna Arts and Science

[Read full review](#) 

“My relationship with Aikido Security is purely as a customer. There is no partnership, no reseller agreement, no referral agreement, and no affiliate relationships of any kind beyond my standard subscription. Everything I shared in this interview is based entirely on genuine, hands-on experience, and my opinions are completely my own..”

B Goswami

Product Manager at Zidio development

[Read full review](#) 

“Before choosing Aikido Security, I evaluated other options such as Checkmarx, Semgrep, and SonarLint. These are in the market, but Aikido definitely performs better than all of them, and its customer support is very good. That's why I chose Aikido Security. I compared online reviews, and Aikido seems to be very promising in that nature, so I chose Aikido Security from my point of view..”

Aman Raj Pandey

Sr. Project Analyst [Cybersecurity] at a consultancy with 10,001+ employees

[Read full review](#) 

“Before choosing Aikido Security, options such as GitHub Advanced Security, Mend.io, and Snyk were evaluated. Each had strengths, but Aikido Security felt simpler to deploy and easier for developers to adopt without extensive training..”

Imyashpatel Patel

Software Developer at Bisag-N

[Read full review](#) 

“I did a thorough evaluation before choosing Aikido Security. I looked at several alternatives. The first one was Snyk, which was my previous tool. Snyk is the market leader in developer security and has excellent dependency scanning. However, the pricing was significantly higher, especially as our repository count grew. Alert noise was also a consistent frustration, with too many false positives requiring manual triage. Aikido Security's Auto-Triage was noticeably better in our testing. The second thing is Semgrep. It is also a very powerful static analysis tool and highly customizable, but the customizability that makes it powerful also makes it complex to configure. For my small team, I needed something that worked well out of the box without significant configuration overhead. Semgrep felt more suited to large security teams with dedicated AppSec engineers. I chose Aikido Security because it is the best one..”

B Goswami

Product Manager at Zidio development

[Read full review](#) 

ROI

Real user quotes about their ROI:

“Aikido Security is an investment that saved my time by automating security checks and helping identify issues early before they become costly problems..”

Abdulmunafz Mct

Full Stack Developer at Sri Krishna Arts and Science

[Read full review](#) 

“You can say we have seen a return on investment in time saved. Regarding pricing, I don't know how much ROI we have saved, but you can say the task, which usually took around seven to eight days, now takes two to three days, hardly three days. Within that, we just complete the task using Aikido Security, so we save around three to four days..”

Aman Raj Pandey

Sr. Project Analyst [Cybersecurity] at a consultancy with 10,001+ employees

[Read full review](#) 

“I have seen a return on investment with time saved. We needed fewer employees because of that as well. We got SOC 2 compliant very fast with Aikido Security. We were expecting to complete the compliance in a month, but I figured out Aikido Security could do it within a week for all our 13 repositories..”

Samir Patil

Co-Founder & CTO at Mango Giraffe

[Read full review](#) 

“The return on investment has come mostly from operational efficiency, as consolidating much of the workflow, previously involving maintaining separate tools for dependency scanning, secret scanning, and code scanning, has saved somewhere between 10 to 15 engineering hours per week across teams handling security reviews manually..”

Imyashpatel Patel

Software Developer at Bisag-N

[Read full review](#) 

“While I cannot talk about money saved because I do not manage any financial decisions or have access to financial information, I can say that we have saved a lot of time. We no longer need our internal automations that were running in our internal Lambda deployments, which were quite slow and needed a lot of maintenance from our engineers. Since we got rid of that, our productivity has increased, I believe, by thirty-two percent..”

Francisco Javier Vergara

SecOps Engineer at IriusRisk

[Read full review](#) 

“The return on investment with Aikido Security was very clear and measurable across multiple dimensions. First and most significant is the cost of prevented breaches. Aikido Security caught a critical remote code execution vulnerability in my Python machine learning pipelines before it reached production. Industry estimates put the average cost of a data breach for a small to mid-sized company at anywhere between one hundred thousand to five hundred thousand dollars. When you factor in incident response, legal costs, customer notification, and reputation damage, preventing even one such incident more than justified my entire annual subscription many times over. The second one is developer time savings. Before Aikido Security, my senior developers spent roughly six to eight hours per week manually reviewing code for security issues and triaging vulnerability alerts from multiple tools. After Aikido Security, that dropped to approximately one to two hours per week, a saving of nearly seventy-five percent of security review time. Across a team of five developers, over a year, that translated to hundreds of recovered engineering hours redirected towards actual product development. The third one is tool consolidation savings. I replaced Snyk and a separate secret scanning tool with Aikido Security alone. That consolidation saved approximately four hundred to five hundred dollars monthly in subscription costs while actually improving our security coverage..”

B Goswami

Product Manager at Zidio development

[Read full review](#) 

Use Case

“I use Aikido Security for identifying security vulnerabilities in code and dependencies and cloud configurations. In my full-stack project, Aikido Security helped to detect the vulnerable packages and security issues before deployment, thereby improving application security. It also provides actionable recommendations that make it easier to fix issues quickly during deployment..”

Abdulmunafz Mct

Full Stack Developer at Sri Krishna Arts and Science

[Read full review](#) 

“Aikido Security has been in use for a little over a year, starting as a security initiative from the engineering side because code was scattered across multiple repositories, making CI/CD pipeline and security fixes a significant problem.

“The main use case for Aikido Security is application security across the development life cycle, primarily for dependency vulnerability scanning, secret detection, and container image scanning, as the goal was not just finding vulnerabilities, but releasing the backend for different developers while still delivering..”

Imyashpatel Patel

Software Developer at Bisag-N

[Read full review](#) 

“I have been using Aikido Security for approximately more than one year, primarily for securing our development pipelines and scanning our codebase for vulnerabilities across multiple projects.

“The use case is definitely developer-first vulnerability management. Aikido Security nests directly in our development workflow and it catches security issues before they reach production. It integrates with GitHub very well. Pull requests get automatically scanned. From that point of view, security becomes part of development rather than an afterthought..”

B Goswami

Product Manager at Zidio development

[Read full review](#) 

“My main use case for Aikido Security is to perform SAST, security code review of codes provided by developers, and SCA determination or dependency checks.

I used Aikido Security during an engagement where I performed SAST on a code to review what flags or vulnerabilities are part of the codebase. I identified many critical and high-level vulnerabilities, which helped to further mitigate those so that in production, there are no such issues.

Additionally, I perform SCA determination with Aikido Security to check that dependencies are not vulnerable in nature, ensuring all are safe and no vulnerabilities are present in the dependencies..”

Aman Raj Pandey

Sr. Project Analyst [Cybersecurity] at a consultancy with 10,001+ employees

[Read full review](#) 

“My main use case for Aikido Security is to utilize it as part of our vulnerability management program, where we also scan our images, codes, and manage our SBOM.

“A specific example of how I use Aikido Security in our vulnerability management program occurs every time new code is pushed into our repositories. Aikido scans for this new code and raises new vulnerabilities within these new codes. Then, with our automations, a Jira ticket gets created, our engineering team takes a look at it, and adjusts security if needed, resolving it within a few days.

“Additionally, we use Aikido Security to generate a current status of our software, and I have created an automation that daily exports all of the vulnerabilities our software has, groups them by severity, and generates a report that can be shared with our customers..”

Francisco Javier Vergara

SecOps Engineer at IriusRisk

[Read full review](#) 

“I used Aikido Security at my previous organization for almost two to three weeks because we had to achieve SOC 2 compliance for our current codebase.

The main use case for Aikido Security was to resolve the vulnerabilities in the packages we were using. I wanted to remove the vulnerabilities from them and update to the latest stable version. A couple of code changes along with package changes were also involved.

Aikido Security helped me with the vulnerabilities and package updates through a simple workflow where I just had to open Aikido Security dashboard, connect my GitHub account, select the repository and scan it. After scanning it, Aikido Security would raise a PR for each vulnerability, specifying what those vulnerabilities were. I would then merge the PR, and it would also run the test cases that I already had attached to my codebase.

Regarding my main use case with the workflow, the process was straightforward. However, there was one minor issue that I faced. When I had a UUID for an object in the code, Aikido Security was considering it as a secret key, which it was not. This was a false positive alarm, but it was not a major issue and merely feedback I wanted to provide..”

Samir Patil

Co-Founder & CTO at Mango Giraffe

[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 setup cost was easier than expected, with pricing feeling reasonable compared to some larger platforms that were evaluated. The bigger cost was licensing if it involved developer time spent reviewing the initial backlog of findings..”

Imyashpatel Patel

Software Developer at Bisag-N

[Read full review](#) 

“My experience with the pricing, setup cost, and licensing was very easy, as all information is already public. They have their pricing tiers publicly available to everyone. We also had help from our customer success manager who was with us the whole way..”

Francisco Javier Vergara

SecOps Engineer at IriusRisk

[Read full review](#) 

“I purchased directly through Aikido Security's website. The signup and onboarding process was very straightforward. Connecting my GitHub organization, I was scanning within minutes, with no complex procurement process needed. Aikido Security's pricing setup follows a repository-based pricing model. The cost scales with the number of repositories being scanned. For small teams, the entire price is very reasonable. The setup cost was essentially zero, with no professional services or implementation fees. The self-service onboarding took less than thirty minutes to connect all repositories and configure scan rules. Licensing is a straightforward annual or monthly subscription, with no per-user fees, which is developer-friendly. Overall, it is one of the most transparent and accessible pricing models I have seen in the security tools space..”

B Goswami

Product Manager at Zidio development

[Read full review](#) 

Customer Service and Support

“Customer support is good; if you raise a query, hardly within a day, your issues get resolved, and designated teams contact you instantly, with tickets getting created and all the tracking happening very smoothly..”

Aman Raj Pandey

Sr. Project Analyst [Cybersecurity] at a consultancy with 10,001+ employees

[Read full review](#) 

“Customer support has been contacted a few times and responses have been generally quick, usually within a business day. The interaction felt technical rather than scripted, which was appreciated. Most issues were resolved through documentation links, configuration guidance, or clarification around findings..”

Imyashpatel Patel

Software Developer at Bisag-N

[Read full review](#) 

“The customer support experience was genuinely positive, especially for a relatively young company. Onboarding support was excellent. Their team proactively reached out after signup to ensure we were set up correctly. Response time for support tickets averaged twelve to twenty-four hours, which is faster than most enterprise security tools. The documentation is clear and well-maintained. Their changelog is also very transparent, with regular product updates and clear explanations. I would rate support an eight out of ten, one of the better support experiences in the developer tools space..”

B Goswami

Product Manager at Zidio development

[Read full review](#) 

“Customer support for Aikido Security is incredibly efficient. I can get an answer to a question within two or three minutes.

“I chose a rating of ten because after reviewing several other products, Aikido Security was the easiest to use, the easiest to onboard, and the one with the most active customer support. I have a Slack channel with them where I can ask whatever I need and they will respond within minutes, which really helps us..”

Francisco Javier Vergara

SecOps Engineer at IriusRisk

[Read full review](#) 

Other Advice

“My advice for others looking into using Aikido Security is that you should give it a try. Aikido Security will resolve all your vulnerabilities quickly, and if you have test cases already written in your branch, it will do a pretty good job. I would rate this solution a 9 out of 10..”

Samir Patil

Co-Founder & CTO at Mango Giraffe

[Read full review](#) 

“Aikido Security saved me several hours each week by automating vulnerability scanning and security checks, reducing the need for manual review and helping me focus on more development.

“If you are starting out, use Aikido Security early in development to catch security issues sooner and build more secure applications. Aikido Security provides strong visibility into security risk, vulnerability management, and compliance-related insights in governance and security. I would rate this product an 8 out of 10..”

Abdulmunafz Mct

Full Stack Developer at Sri Krishna Arts and Science

[Read full review](#) 

“Advice to others looking into using Aikido Security is to avoid connecting everything at once, as more findings than expected will likely be uncovered. Starting with critical repositories, establishing a remediation process, and defining ownership early can prevent teams from getting overwhelmed by the

alert volume. Also spend some time tuning the policies before rolling it out company-wide.

“Integrating Aikido Security as a single tool reduces much manual effort that used to occur around vulnerability management. The overall review rating for Aikido Security is 8 out of 10..”

Imyashpatel Patel

Software Developer at Bisag-N

[Read full review](#) 

“Regarding Aikido Security's accuracy and reliability of output, I can say its reliability is 80 to 90%. It definitely works and delivers very good results, easily identifying if you need clarification with the type of vulnerability it has identified and providing a more detailed review of each of them.

If a person is looking for a SAST, DAST, and a complete combination of a pack of security tools, then Aikido Security is best. It helps to perform SAST, DAST, which is dynamic application testing, and most tools don't combine all of them in one. You can also scan your cloud and your infrastructure as code things, covering all the wide areas of your project, so that type of person can definitely choose Aikido Security.

I would rate my overall experience with Aikido Security as an 8 out of 10..”

Aman Raj Pandey

Sr. Project Analyst [Cybersecurity] at a consultancy with 10,001+ employees

[Read full review](#) 

“Since switching to Aikido Security, I have noticed a positive impact on my team's

productivity with measurable results, as we now have measurements. Before, we did not even know how many vulnerabilities were raised per new functionality. We lacked a lot of visibility because reporting of vulnerabilities was not automated. New vulnerabilities were being raised by our automations, but tickets were not created automatically. We have gained a lot of productivity by not having to review the vulnerability reports themselves, but only needing to review the Jira tickets, which makes it much easier for our engineers.

“My advice for others looking into using Aikido Security is to invest time in reading their documentation, as Aikido Security functionality can be exploited very much. I would rate this review a ten overall..”

Francisco Javier Vergara
SecOps Engineer at IriusRisk

[Read full review](#) 

“I have several practical pieces of advice for anyone considering Aikido Security. The first one is to connect all repositories from day one, not just your main production ones. Security vulnerabilities hide in unexpected places such as internal tools, side projects, and experimental repositories. Full coverage from the start gives you complete visibility. The second one is to spend time configuring Auto-Triage rules early. The default settings are good, but customizing triage rules for your specific tech stack significantly reduces noise. Invest that configuration time up front, and you will thank yourself later. The third one is to integrate with your existing workflow immediately. Connect Aikido Security to your GitHub pull request process from day one. [Make](#) security scanning a non-negotiable part of every code review. If you add it as optional, it will get ignored. Use it as a developer education tool. Aikido Security does not just find vulnerabilities; it explains why they are dangerous. Encourage developers to read those explanations. Over time, our entire team's security knowledge improved naturally. I would rate this product an eight out of ten overall..”

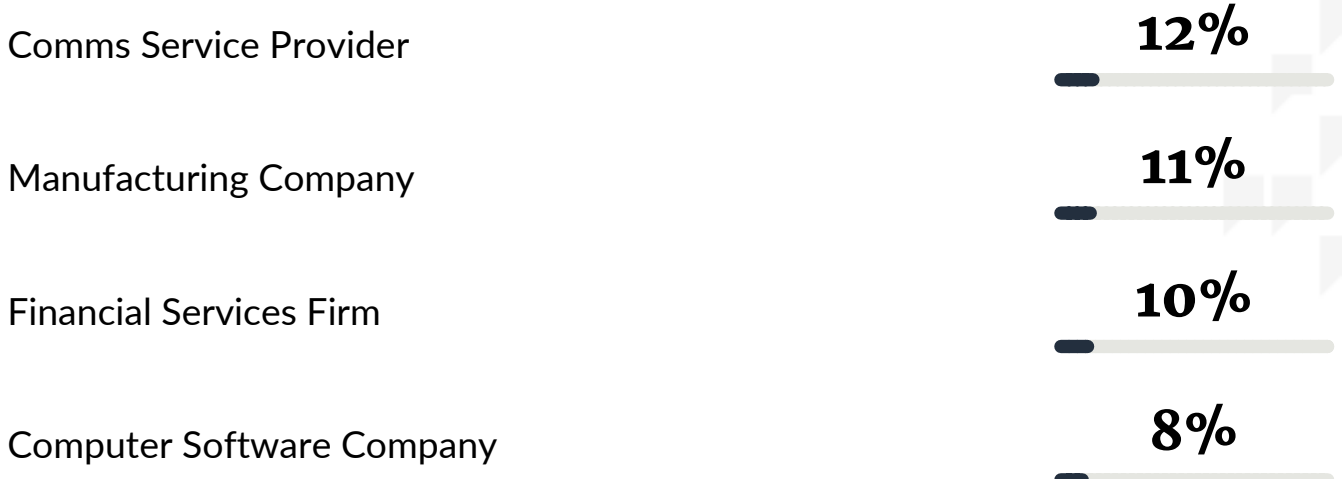
B Goswami

Product Manager at Zidio development

[Read full review](#) 

Top Industries

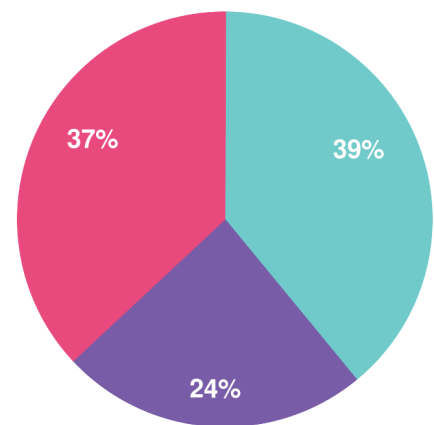
by visitors reading reviews



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 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