aws marketplace

Devo

Reviews, tips, and advice from real users

Contents

Product Recap

Devo

Devo Recap

Devo is the only cloud-native logging and security analytics platform that releases the full potential of all your data to empower bold, confident action when it matters most. Only the Devo platform delivers the powerful combination of real-time visibility, high-performance analytics, scalability, multitenancy, and low TCO crucial for monitoring and securing business operations as enterprises accelerate their shift to the cloud.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

✔ "The most useful feature for us, because of some of the issues we had previously, was the simplicity of log integrations. It's much easier with this platform to integrate log sources that might not have standard logging and things like that."

JohnBusch

Security Engineer at Kforce

✔ "It centralizes security management within a business, functioning as a core system for a SOC."

Michael Wenn

CEO / Co-Founder at Aiops ltd

✔ "The alerting is much better than I anticipated. We don't get as many alerts as I thought we would, but that nobody's fault, it's just the way it is."

Verified user

IT Risk Manager at a recreational facilities/services company with 501-1,000 employees

✔ "Devo helps us to unlock the full power of our data because they have more than 450 parsers, which means that we can ingest pretty much any type of log data."

KevinGolas

Director of World Wide Security Services at Open Text

✔ "Those 400 days of hot data mean that people can look for trends and at what happened in the past. And they can not only do so from a security point of view, but even for operational use cases. In the past, our operational norm was to keep live data for only 30 days. Our users were constantly asking us for at least 90 days, and we really couldn't even do that. That's one reason that having 400 days of live data is pretty huge. As our users start to use it and adopt this system, we expect people to be able to do those long-term analytics."

Verified user

Product Director at a insurance company with 10,001+ employees

✔ "Devo provides a multi-tenant, cloud-native architecture. This is critical for managed service provider environments or multinational organizations who may have subsidiaries globally. It gives organizations a way to consolidate their data in a single accessible location, yet keep the data separate. This allows for global views and/or isolated views restricted by access controls by company or business unit."

Gabe Martinez

CEO at Analytica 42

✔ "In traditional BI solutions, you need to wait a lot of time to have the ability to create visualizations with the data and to do searches. With this kind of platform, you have that information in real–time."

Verified user

Digital Security VP at a tech services company with 201-500 employees

What users had to say about valuable features:

"I am a sales and technical support engineer, and Devo has a really good website for creating custom configurations. I can easily create a customized server with their website, so it's a great product for sales engineers.."

César-Rodríguez

Works at a construction company with 51-200 employees

Read full review ⬈

"The most valuable feature of the solution is the log retention time. The dashboarding, what Devo calls Activeboards, is a very useful feature enabling rendering a range of insights from data and related detections. Devo enables collaborative working across security teams within the platform.."

Verified user

Director at a security firm with 51-200 employees

Read full review ⬈

"The alerting is much better than I anticipated. We don't get as many alerts as I thought we would, but that nobody's fault, it's just the way it is.

Having at least one year of data was one of our requirements, so 400 days of hot data benefits us. We are used to this capability, as our previous solution offered the same, and we wouldn't have purchased Devo if it didn't provide that. ."

Verified user
IT Risk Manager at a recreational facilities/services company with 501-1,000 employees

Read full review ↗

"One of Devo's standout features is its cloud-first architecture, which sets it apart from many traditional SIEM providers that still rely on legacy, on-premise solutions. While many companies have started shifting to the cloud, Devo offers a hybrid solid approach with full cloud deployment. This mature architecture is one of Devo's significant strengths. Unlike other providers like Fortinet and Sentinel, which handle specific security parts, Devo offers a more comprehensive, end-to-end solution, making it one of the most advanced SaaS products.."

Michael Wenn
CEO / Co-Founder at Aiops ltd

Read full review ↗

"The querying and the log-retention capabilities are pretty powerful. Those provide some of the biggest value-add for us.

We also find their Activeboards, which are their dashboards, useful for just displaying data and seeing historical trends.

We also use their alerting capability to a limited degree, although we don't really have too much invested in alerting yet.."

Verified user   Read full review ↗
Director of Security at a tech company with 501-1,000 employees

" The most useful feature for us, because of some of the issues we had previously, was the simplicity of log integrations. It's much easier with this platform to integrate log sources that might not have standard logging and things like that.

Alerting is very easy to set up and use, and it's pretty robust. It takes a lot of ingests. We had some issues previously where we were overwhelming our old SIEM. We were setting too many logs, and it couldn't handle the load. That's why we looked for something that could have much higher rates of ingestion.

The fact that the solution manages 400 days of hot data was a huge selling point. In our organization, we have to have 365 days of hot data all the time, and licensing that with other solutions was extremely expensive. ."

JohnBusch   Read full review ↗
Security Engineer at Kforce

Other Solutions Considered

"Devo is the first SIEM for us. We didn't have anything before this. We're growing as an organization, and SIEM in general, and Devo in particular, let us scale up our capabilities without having to scale up our manpower.."

Verified user   Read full review ↗
Director of Security at a tech company with 501-1,000 employees

"We focused on four solutions: Splunk, AlienVault OSSIM, the incumbent QRadar, and Devo. We narrowed it down pretty quickly to Splunk and Devo, and the latter was a bit cheaper, though less mature. We took a chance and went with Devo.."

Verified user   Read full review ↗
IT Risk Manager at a recreational facilities/services company with 501-1,000 employees

"We looked at seven different competitors. We looked at Splunk. We looked at Sentinel. We looked at LogRhythm, and we reviewed the newer McAfee SIEM. We did our due diligence. We looked at a lot of them. We did a POC on LogRhythm as well as Sentinel and Devo. We did a bake-off, and Devo was the clear leader.."

JohnBusch   Read full review ↗
Security Engineer at Kforce

"We previously used IBM QRadar, and we switched because it was antiquated. We had difficulty ingesting logs from cloud solutions, which is the direction our organization is moving in. We have several cloud solutions now versus two or three years ago, so the migration to Devo from QRadar was very timely for us in that regard.

QRadar's interface was pretty antiquated. They have updated it now, but we weren't satisfied with it at the time. We also had some support-related issues around updating the solution as it was on-prem. We were coming to a point where we had to update the hardware and software, so it was a good time for us to look for another product.."

Verified user
IT Risk Manager at a recreational facilities/services company with 501-1,000 employees

Read full review [↗]

"We used McAfee Nitro. We switched because the technology was very slow and outdated. It wasn't keeping up with the times. Keeping the 365 days of hot data was getting extremely expensive and cumbersome because of the number of disk resources we had to throw at it. The support and updates to the platform were manual because it was an on-prem solution. So, anytime we had to do a major rollout of a SIEM upgrade, it took hours, and it was always problematic, whereas, with a SaaS solution, it's just done in the backend for us.

Implementing Devo has helped reduce blind spots versus our previous SIEM solution especially when it comes to cloud products. McAfee Nitro SIEM had pretty much zero cloud connectivity. We're pretty heavy with Azure and M365 stack, and they had no connectors to get any of those logs into our SIEM. So, we were completely blind to our cloud products.

The biggest impact is that we're able to proactively recognize issues that we're having in those cloud environments. Previously, they were either discovered by somebody accidentally, or an issue arose or an incident happened and we had no alerting around it. We had to triage afterward, whereas now, we have alerting. So, we get those alerts ahead of time.."

JohnBusch
Security Engineer at Kforce

Read full review ↗

"We definitely looked at competitors, the standard players in this space: Splunk, LogRhythm, and others. We ended up choosing Devo because of two or three things.

First, as an organization, they were very responsive. The support, even during our PoC and evaluation process, and afterward, was and continues to be phenomenal. We know that they're a smaller company like us, and it felt like they were more attentive to us as customers.

The second factor was the price point. If we had to stand up similarly sized solutions from some of the other vendors, it would be much more expensive.

And one of the biggest reasons we went with Devo was that we're a small security team, and we didn't want to have to manage SIEM infrastructure. Devo meets that requirement for us because it's SaaS. There are other SaaS SIEMs, but Devo seemed like the best. All we had to do was pump logs. With other platforms there are infrastructure aspects, like storage and indexers that you have to worry about. We don't have to do any of that. We just put in the logs that we want, up to a limit, and that's it. It allows us to focus on getting the actual value-add out of the logs, rather than spending a lot of bandwidth managing the infrastructure.."

Verified user   Read full review ↗
Director of Security at a tech company with 501-1,000 employees

ROI

Real user quotes about their ROI:

"Devo allows us to ingest more data compared to other solutions, using the same infrastructure. For example, compared to Splunk using the Capacity Planning Tool, Devo can ingest almost double the information in terms of events per second.."

Verified user   Read full review ↗

Digital Security VP at a tech services company with 201-500 employees

"As is often the case with security solutions, it's hard to measure an ROI because we only need it once an incident occurs. The hope is that we get a return if an incident takes place. Devo is much better than we previously had, but it's also a lot more expensive, so it should be so.."

Verified user   Read full review ↗

IT Risk Manager at a recreational facilities/services company with 501-1,000 employees

"More than anything, we have seen ROI in the amount of time saved during investigations. From that perspective, it has paid for itself.

Within the first quarter after we started using it, there were incidents that Devo was able to help us quickly assess and investigate. As a tool, it showed its value pretty quickly.."

Verified user
Director of Security at a tech company with 501-1,000 employees

Read full review ↗

"We have absolutely seen an ROI. We've been able to hire one more analyst with the money we saved on our licensing.

We extracted value within the first two weeks because we were able to ingest our cloud solutions, but at the 60 to 90 day point, we 100% realized our investment, and we were completely satisfied.."

JohnBusch
Security Engineer at Kforce

Read full review ↗

"I have seen a return on investment, and without disclosing figures, I can put it in terms of capabilities. This product allows us to scale up the way we need to, without any additional costs, or there's already a fixed cost with that. This is key for us.

We can bring in any size of customer, from the smallest client to the largest company. Also, I have been able to bake in the pricing model to adjust to the margin that I need for a specific customer.."

KevinGolas
Director of World Wide Security Services at Open Text

Read full review ↗

"Devo saves us time. The turn-up time for the cloud is very quick with their SaaS infrastructure. Getting data in is relatively quick, whether it is leveraging relays, collectors or both. They are very modern in the sense that they are very friendly with GCP, AWS, Azure, etc., in terms of just needing plugin API keys, then it will start ingesting data and parsing it.

They have easy to configure Relays that can go on-prem and pretty much collect any type data that you can think of. I have always been very happy with that. It is a joy to partner and be able to work with this kind of system.

If you have acquired different data stores or SIEMs over time, especially if you are a large organization, you find yourself buying one of each. That is kind of wasteful, inefficient, and expensive. Because of the Devo's scalability and low-cost, you can get the data from all those disparate environments into one place. Additionally, a lot of times in those environments, you have to filter out data so the systems don't get overwhelmed, thus you are partially blind on things you do not collect. With Devo, their philosophy is you can go ahead and collect all the data. Devo's ROI is saving on redundant licensing costs, storage/processing costs, collection costs, overhead of maintenance cost, but more importantly the ability to build a more holistic security program because you visibility to all your data for 400 days. This helps any organization for detection and compliance reasons.."

Gabe Martinez   Read full review ↗
CEO at Analytica 42

Use Case

"Devo is a SIEM replacement technology used to run security operations. It centralizes security management within a business, functioning as a core system for a SOC. This system is the central cybersecurity hub, helping manage and streamline service tickets.."

Michael Wenn   Read full review ↗
CEO / Co-Founder at Aiops ltd

"During the pandemic, small and medium companies didn't buy big servers. Latin American countries only used Devo in industries, maybe banks or security government projects. We create server appliances, such as servers plus switches.."

César-Rodríguez   Read full review ↗
Works at a construction company with 51-200 employees

"Our primary use case is so we have historical logs in case of an event or if we need to do any troubleshooting.

Our secondary use of Devo is for incident detection; certain logs trigger alerts, so we now have a 24/7 monitoring service that detects and alerts us to incidents. ."

Verified user

IT Risk Manager at a recreational facilities/services company with 501-1,000 employees

[Read full review](#) ↗

"We are an MSSP and we provide security monitoring services for our customers. We also treat ourselves as a customer. That means we use Devo internally for our own services in addition to using it to monitor our customers. The use case varies by customer, but they are all security-related as well as dealing with a little bit of storage retention, depending on the customer's needs.."

Verified user

Director of Security Architecture & Engineering at a computer software company with 51-200 employees

[Read full review](#) ↗

"We're mostly using it for log retention and investigations into events or security issues within our environment. We're pumping a lot of the logs from our SaaS tools into it, from tools like Google Workspace (G Suite) and OneLogin and the like. When we have questions or investigations from a security perspective, we go into Devo to help answer them.."

Verified user
Director of Security at a tech company with 501-1,000 employees

Read full review ↗

"We have most of our major log sources going to it, and we have both an internal NOC as well as an external MSSP that does 24/7 monitoring. We use it for writing all of our alerting use cases for different correlations between all of our different logging apps.

In terms of our environment, we have several departments. We're a staffing company, and we have a lot of different contractual obligations with other companies. So, it's a fairly complex environment. We have multiple domains. We have several DMZ environments, and we have three active data centers.."

JohnBusch
Security Engineer at Kforce

Read full review ↗

Setup

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

"The initial setup was relatively straightforward.

In terms of maintenance, I go through every quarter to ensure that each of our log sources is still sending logs to Devo. We were a little disappointed that they didn't have a good way of informing us if a log source stopped sending logs. I appreciate that each source sends on a different frequency, but we should be able to define that frequency and receive a notification of any issues.."

Verified user

Read full review ↗

IT Risk Manager at a recreational facilities/services company with 501-1,000 employees

"The setup phase required technical input and that increases with the scale of the project, but Devo are willing to assist.

The solution is deployed in Devo's cloud. It is possible to get Devo on-premises, but that is not the main offering.

Deploying Devo you can get the right security outcomes within a few weeks to a month. Its heavily dependent on the scope of the solution.."

Verified user   Read full review ↗

Director at a security firm with 51-200 employees

"We have two options with the initial setup. One is we buy the chassis from the OEM and customize the server. I prefer the OEM server because we have a customized image-focused VLAN, so it is easier for the integrator or customer to set it up. You just need to open the box, turn the server on, and they are ready to install the DNS software.

We have another option where we resell only the Devo server. We are just starting to do this, and it is not easy to assemble because we need a lot of skill.

The time taken to deploy Devo depends. If the final customer has everything done, or if everything is correctly installed, the rack, the air conditioner, or the UPS, it takes two to three hours at most to customize the server and the network card. We need two or three people for labor when the integrator installs the server. We need just one person to configure the server.."

César-Rodríguez   Read full review ↗

Works at a construction company with 51-200 employees

"The complexity comes from getting the data sources ingested. There are some easy ones for common tools like Google or OneLogin or AWS. Getting the logs of those big SaaS tools into Devo was not too difficult. But there are a lot of SaaS tools out there and, especially in the beginning, Devo had to create custom collectors and parsers for us for some of the smaller ones, and that took a while to do.

In terms of getting our staff up to speed on using the solution, on a scale of easy to difficult, it was in the middle. The basic functionality, especially the dashboards and where the data is, is not that difficult. Where the complexity comes in is when it comes to getting value out of that data. There's a query language, called LINQ, which is SQL-like but has quirks that are Devo-specific. That takes some time to learn, but that would probably take time on any platform. Overall, the learning curve is not really easy, but it's not really that difficult either.."

Verified user   Read full review ↗

Director of Security at a tech company with 501-1,000 employees

"The initial setup is easy. They have a lot of out-of-the-box integrations and are quite lightweight in their implementation. There are plenty of options for integration, which I would consider one of their strengths. One standout feature beyond data analytics and real-time diagnostics is something called DeepTrace. If I recall correctly, this feature involves automated threat hunting and investigation. It uses AI to expedite the investigation process, identifying attack chains and conducting root cause analysis without human intervention. Essentially, they're using AI to perform tasks typically done by analysts, automating the investigation process. When you start an investigation, their AI-driven tool provides the best guess at identifying the problem, potentially offering root cause analysis without human involvement. You can either use their suggested analysis or investigate further if needed. This DeepTrace feature is likely one of the unique selling points of their platform, making it a significant differentiator for them.

I rate the initial setup an eight out of ten, where one is difficult and ten is easy.."

Michael Wenn
CEO / Co-Founder at Aiops ltd

Read full review ↗

"I led the deployment project. Any project is complex to a degree, but it was as straightforward as they could make it.

In terms of the implementation strategy, we mapped out everything. We had a corporate-wide project around it. The Devo team was completely a part of the deployment project along with our third-party MSSP. The three teams worked together through the entire project. From Devo's side, Rory gave us a hand. Yailin Perez was great. William Wilde was really good. He's a great engineer over there.

The migration piece wasn't bad at all. The initial build-out was a little bit cumbersome, but that goes with any system. For standing up the relays, endpoint managers, and things like that, there was some lead time. It took us about three months just to get everything built and in place for our on-prem pieces to send the information to Devo, but once we were up and rolling, we moved all of our log sources and all of our alerting in just over 90 days.

The ease of migration was extremely important because we were very close to the end of our licensing with our previous SIEM, and we didn't want to relicense and pay for support if we didn't have to. We were able to migrate quickly and avoid that expense.

Devo's team was with us every step of the way. We had weekly stand-ups three times a week, and anytime we reached out to them, they jumped on a call with us immediately. They gave us really good first-line support, and their professional services team was great. They were very knowledgeable, and they assisted us a lot. Our experience was great.

It wasn't difficult at all to get our staff up to speed on using the solution. They provided us with some free training and most of our teams took the free training. So, we were able to hit the ground running as soon as we had the solution in place.."

JohnBusch   Read full review [↗]
Security Engineer at Kforce

Customer Service and Support

"Once we get a hold of someone and they respond, customer support is fine. It isn't extraordinary, and the escalation process is a little below average for the industry.."

Verified user
IT Risk Manager at a recreational facilities/services company with 501-1,000 employees

Read full review ↗

"The community support is excellent. I rate the direct support around eight, mainly because the company is based in America and has more support infrastructure there than in Europe. In the U.S., the support level rating should be closer to ten.."

Michael Wenn
CEO / Co-Founder at Aiops ltd

Read full review ↗

"I like their technical support. They respond in one business day, and they are always available. I always do the first level of technical support, but if I need to solve something quickly, and if the problem is hardware, Devo might send, for example, a power supply or a technician to change something.."

César-Rodríguez
Works at a construction company with 51-200 employees

"I have contacted them a couple of times. T hey were great. They were quick to assist us. Two different times, we were hitting some issues that were rather complex, and they jumped on calls with us, and we were able to resolve them.."

JohnBusch
Security Engineer at Kforce

"Their tech support has been great, once we've raised issues with them. They've been pretty responsive and I'm pretty happy with that part.

Whenever we've opened a ticket, especially when it's been high-priority, they've responded fairly quickly. They're certainly friendly and they try to be helpful, within the limits of whatever they can do. They also escalate quickly if it looks like it's not getting to a solution within the purview that they have.."

Verified user
Director of Security at a tech company with 501-1,000 employees

"Support is pretty good. They're responsive and they usually solve problems relatively well. And if they mess something up, they will actually put professional services people in to solve the problems, if a wide range of issues is involved.

Both our technical and channel-partner relationships have been very good. We meet with them for status calls at least twice a month. They're very good about staying in contact to provide both satisfaction and technical assistance.."

Verified user

Director of Security Architecture & Engineering at a computer software company with 51-200 employees

Read full review ↗

Other Advice

"We plan on using the Devo Exchange. It's a pretty new feature. Part of the constraints, for us, has been manpower. Our organization is growing pretty rapidly, and we're working on hiring to keep Devo up to date. We just haven't had the bandwidth to invest more into exploring all the features yet.."

Verified user
Director of Security at a tech company with 501-1,000 employees

Read full review ↗

"It is important with any SIEM deployment cloud-based or otherwise to have an experienced implementation team. The implementation team should be prepared to engage closely with the SIEM vendor to get the best from the scope of the deployment.

Overall, I rate the product an eight out of ten.."

Verified user
Director at a security firm with 51-200 employees

Read full review ↗

"Definitely take a good, hard look and considerate it. It's the fast-growing leader in the SIEM field.

Overall, Devo is awesome, but it's got some room to grow. I would like to see better native ingestion of cyber threat intelligence and building out of deeper correlation capabilities. They have some work that they're doing in Flows to do some of that stuff, but it still has room for some additional maturity.."

Verified user
Security Operations Center (SOC) Director at a tech company with 51-200 employees

Read full review ↗

"The biggest thing that we were very careful about was figuring out what our ingest level is ahead of time. It can be very difficult to reach that conclusion, especially when native SIEMs or legacy SIEMs do more ingest on logs per second or events per second, whereas Devo ingests using gigs per day. So, spending some time to figure out that calculation so that you don't over-license or under-license is critical. We were very lucky, and we hit those numbers, but a primary concern of ours at the beginning was making sure we didn't under-license. You don't want to have to expand your licensing and go back to ask for more money.

The biggest lesson that I've learned from using this solution is the way they do the ingest. You don't have to categorize the data ahead of time before ingestion. You can throw all the logs you want at it and then go back and do a correlation afterward. That's the biggest thing we learned. It's a great solution and most other SIEMs don't do that.

Overall, I'd rate it a nine out of ten.."

JohnBusch
Security Engineer at Kforce

Read full review ↗

"It integrates several critical components, such as SIEM, SOAR, and UEBA, to make it a robust solution for SOCs. The platform's cloud-based architecture ensures excellent performance, scalability, and quick deployment, particularly beneficial in environments with heavy production loads or when integrating additional tools.

Devo provides near-real-time capability for threat alerts, analysis, and updates. This allows SOC teams to stay on top of security incidents as they happen. Additionally, the platform excels in visualization, providing clear and timely dashboards that help SOCs avoid missing critical incidents or failing to interpret data correctly. Its user-friendly design allows for high-level overviews and detailed drill-downs, ensuring security professionals can quickly grasp the situation and act.

They push AI as their differentiation, calling it a next-gen SIEM. It offers a more inclusive platform that delivers end-to-end security for the entire customer. Using some weighting system, they use AI to drive down false positive rates by determining whether something is a real threat. They have an AI-powered system that assesses if an issue is real, though the specifics of how it works are difficult to explain. This includes machine learning and algorithms designed to identify complex issues, with some of that learning built into the tool. However, this is pretty standard for most SIM platforms today. The biggest challenge for SIEMs has been to make the information they present smarter and more context-heavy. This is not a differentiation but rather being on par with other AI-driven platforms that aim to reduce false positives and minimize manual checks.

I 100% recommend the solution. It can help most medium to large enterprises develop their IT capabilities to advance quickly. However, if you're already at the top of your field and willing to invest heavily, some pedigree products might offer a ten out of ten experience, but that would be due to the higher cost and specialized features.

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

Michael Wenn
CEO / Co-Founder at Aiops ltd

Read full review ↗

"I rate the solution seven out of ten.

Devo's cloud-native SIEM increased our threat visibility, though we had hoped for a bit higher. Visibility is critical, as we rely upon knowing about security incidents as soon as possible. We expected the solution would provide additional insight, but we're finding it isn't. Devo gives us the historical logs, a fantastic capability we are very happy with. However, the incident and threat detection is not what we had hoped for. Regarding security operations, the tool is different from what we wanted.

Getting our staff up to speed with the solution was right in the middle in terms of difficulty. It wasn't as easy as we had hoped, but it wasn't insurmountable by any stretch of the imagination. Devo provided us with several training sessions, and I wonder how much that helped because our group is very technical. The tool's interface is intuitive, so our staff can find what they need. With regular use, the learning curve is relatively low, but without that, it can take some getting used to, as with any solution. Devo is broad and encompassing, so it requires familiarity to leverage it fully. We don't have dedicated internal staff to manage the solution, so we outsourced the monitoring to an MSP.

The migration from QRadar to Devo was relatively straightforward and painless; we essentially cut the cord on QRadar, maintained the logs and moved them over to the new solution. The ease of migration was relatively important, the old solution was antiquated, so we expected any newer tool to be better.

Migrating the bulk of the initial logs took about three months. We got some aspects up and running during a proof of concept while we were still using the old solution. Once we went live, we migrated the POC environment to a production environment, so it was much less stressful than it could have been.

The Devo team was intimately involved in the migration. They weren't as responsive as we had hoped, and they seemed new and didn't completely understand the product. We received better support on escalation; overall, they were critical to the migration.

Before going down this path, I advise potential customers to document their log sources and what information they need based on their use cases.."
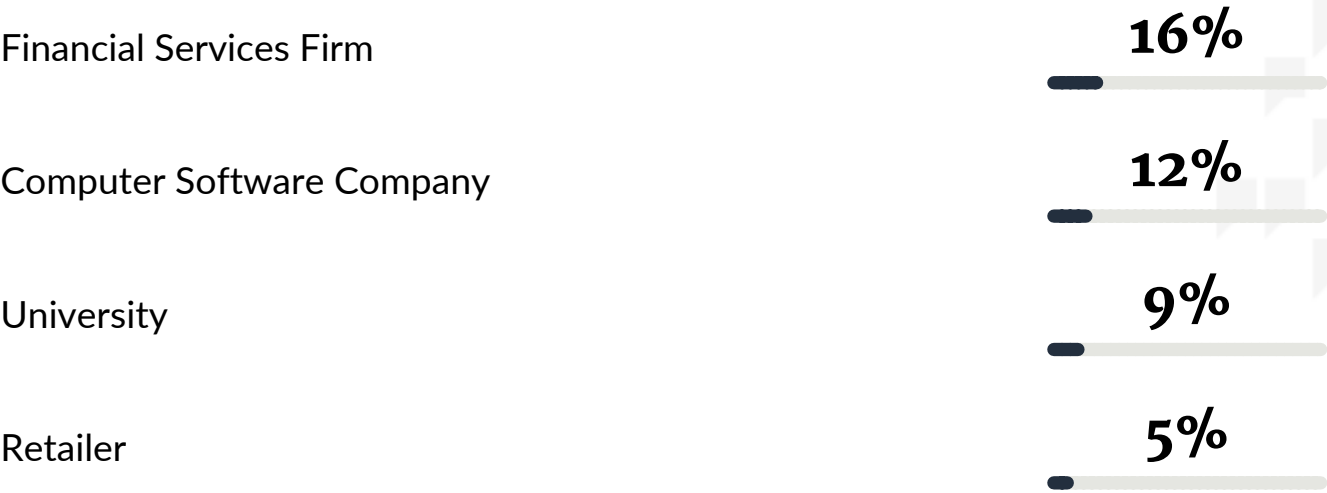
Read full review ↗

Top Industries
by visitors reading reviews

Financial Services Firm

16%

Computer Software Company

12%
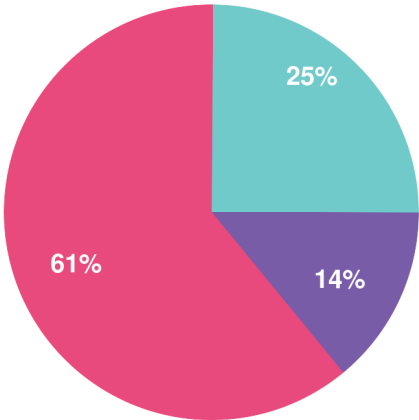
University

9%

Retailer

5%

Company Size

by reviewers
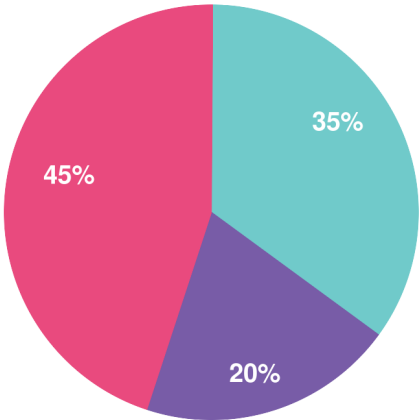
by visitors reading reviews

● Large Enterprise　　　● Midsize Enterprise　　　● Small Business

About this buyer's guide

Thanks for downloading this PeerSpot report.

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

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

Please note that this is a generic report based on reviews and opinions from the collective PeerSpot community. We offer a customized report of solutions recommended for you based on:
- Your industry
- Company size
- Which solutions you're already considering

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

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

Get your personalized report here

About PeerSpot

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

PeerSpot helps tech professionals by providing:

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

Use PeerSpot to:

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

Join PeerSpot to connect with peers to help you:

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

Visit PeerSpot: www.peerspot.com

PeerSpot

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

reports@peerspot.com

+1 646.328.1944