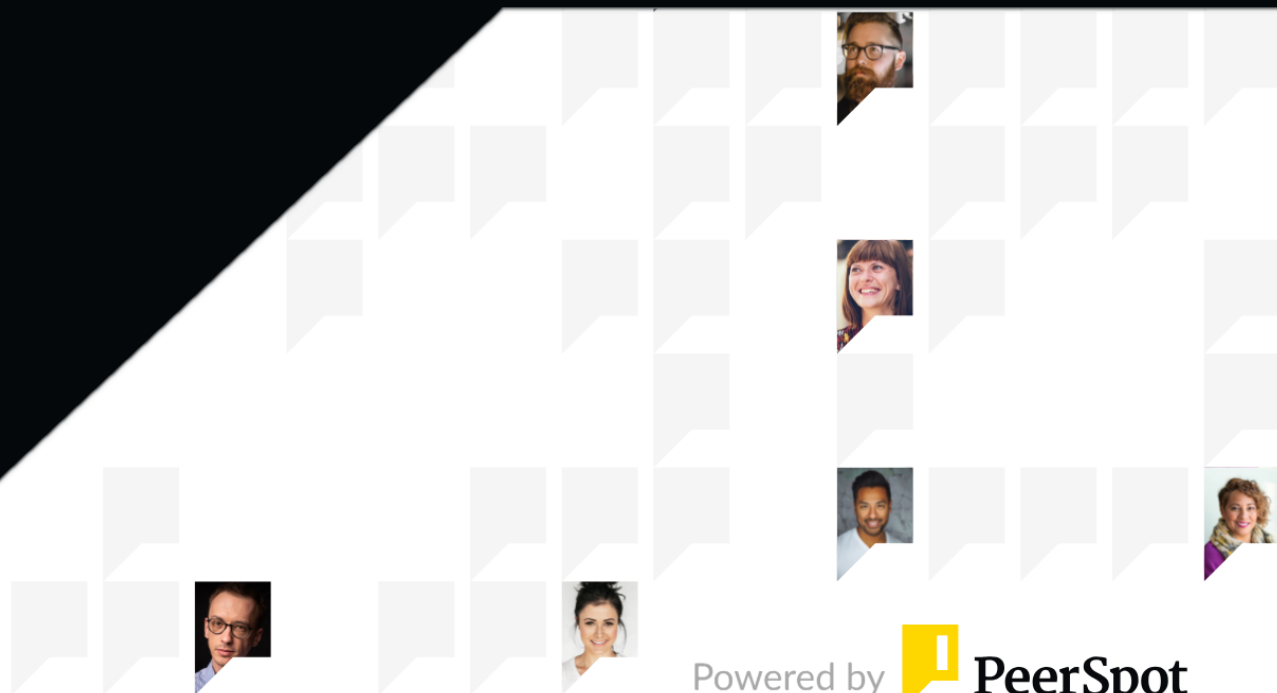


aws marketplace

Devo

Reviews, tips, and advice from real users



Powered by  PeerSpot

Contents

Product Recap..... 3 - 4

Valuable Features..... 5 - 11

Other Solutions Considered..... 12 - 14

ROI..... 15 - 17

Use Case..... 18 - 22

Setup..... 23 - 27

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

Other Advice..... 31 - 34

Trends..... 35 - 36

About PeerSpot..... 37 - 38

Product Recap



Devo

Devo Recap

Devo offers powerful visual analytics, real-time data querying, and log integration capabilities within a cloud-native, multi-tenant architecture, supporting extended data retention ideal for long-term analysis and compliance.

Devo is recognized for its Activeboards, which facilitate visual analytics. High-speed search capabilities and real-time analytics enable efficient data manipulation and querying. Its multi-tenant architecture supports effective data segregation and customization tailored to distinct business needs, enhancing its value for handling complex log integrations. With extended data retention of 400 days and a cloud-native architecture, Devo is a robust platform for long-term analysis and compliance requirements. Though opportunities exist to improve browser stability on large searches, SOAR integrations, and its parser capabilities, Devo remains essential for incident response and security monitoring, offering centralized data storage and analysis.

What are Devo's most important features?

- **Activeboards:** Facilitate visual analytics and data exploration.
- **High-Speed Search:** Enables fast data querying and manipulation.
- **Real-Time Analytics:** Supports instant insights and decision-making.
- **Multi-Tenant Architecture:** Allows effective data segregation and customization.
- **Extended Data Retention:** Offers 400-day log retention for compliance and analysis.
- **Complex Log Integration:** Handles intricate data sources effortlessly.

What benefits and ROI should organizations look for in reviews?

- **Visual Insights:** Enhance understanding through interactive dashboards.
- **Performance Efficiency:** Saves time with high-speed data search and real-time results.
- **Customization Flexibility:** Fits specific business requirements with multi-tenant architecture.
- **Long-Term Compliance:** Ensures alignment with extended data retention needs.
- **Centralized Monitoring:** Enables comprehensive incident response and security monitoring.

Devo is extensively used in industries focused on incident response and digital forensics, centralizing data for security monitoring across hybrid environments. Organizations benefit from its ability to store and analyze aggregated logs, creating alerts and dashboards to enhance visibility for network and endpoint activities in multi-domain settings.

Valuable Features

Excerpts from real customer reviews on PeerSpot:



“The features I find most valuable in Devo are that it works on unstructured data.”



Usama Khan

Team Lead Soc at a tech services company with 51-200 employees



“Devo has the best features for us because we store close to two terabytes a day of data, and it has come in handy for that as I don't find the system to really lag.”



Leland Austin

Senior Consultant and Technical Lead at a financial services firm with 10,001+ employees



“The drill-down reports capabilities allow analysts to click on any element in a widget. When they see a spike in a line chart for a failed login, which could be a true or false attempt, they can click that spike, and a table widget on the same active board instantly populates with raw logs of data for those specific failed logins.”



Francisco Javier Romo

Strategic Account Executive at a computer software company with 51-200 employees



“Devo has positively impacted our organization because we have been using only one tool for our centralized logging systems.”



G Srivastava

Senior Cloud Engineer at a tech services company with 201-500 employees



“Devo has improved our visibility, log management efficiency, and investigation capabilities positively.”



Vikram Chakravarthy

Cyber Security Engineer II (Vulnerability & Threat Management) at FICO



“When comparing Devo with Splunk and Carbon Black, I think Devo is the leader.”



Ahmad Zakwan

Principal Consultant at Syntx Sdn Bhd



“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.”



John Busch

Security Engineer at Kforce

What users had to say about valuable features:

“Integration is easy, and Devo integrates with most products. Devo has connectors that enhance integration with third-party tools such as firewalls and servers.

“Querying helps my data analysis, and it is quite fast. The product provides insight and analytics, and the visualization part contributes to how I understand data insights..”

Ahmad Zakwan

Principal Consultant at Syntx Sdn Bhd

[Read full review](#) 

“In my experience, Devo has the best features for us because we store close to two terabytes a day of data, and it has come in handy for that as I don't find the system to really lag. It's been pretty reliable for us in that way, and with a lot of different types of servers, just to sum it up, let's say Windows, Linux, database, mainframe, etc., sending logs into there, it's pretty easy to find the table that you're looking for when you want to search a query or when a security investigation does come up.

“Devo makes it easy to find the tables or search for queries, especially during a security investigation. However, I don't want to give too much detail because I don't want to be a security risk. If an account has been compromised, you can do a search on the box.unix.rhel table, for example, and then there's a user field or an IP field. You can try and trace it down that way, and it does give you customizable date ranges. You can do real-time, 15 minutes, one hour, 24 hours, or go back a few months, so it allows you to trace it..”

Leland Austin

Senior Consultant and Technical Lead at a financial services firm with 10,001+ employees

[Read full review](#) 

“The best features Devo offers include its focus on security investigation as a SIEM tool. Our SOC and NOC teams mainly depend on this tool for security operations and data analytics. For them, this tool is the main foundation for their daily work, which I believe is a key feature for Devo.

“Devo stands out for our SOC and NOC teams compared to other tools such as Elastic because of its SIEM capabilities for threat detection and investigation. It utilizes 400 days of hot data, allowing queries to run very fast and yield results quicker than other tools in terms of security and SIEM capability. The 400 days of long-term data retention for searchable log data without transitioning to cold storage is significant. If data moves to cold storage, it takes time to retrieve it into hot storage, but Devo provides hot data for 400 days. The security orchestration is an exceptional feature of Devo for our SOC and NOC teams..”

G Srivastava

Senior Cloud Engineer at a tech services company with 201-500 employees

[Read full review](#) 

“The features I find most valuable in Devo are that it works on unstructured data. That is the thing that I appreciate about it. It works on the LINQ query, which is similar to SQL syntax. I appreciate this aspect about it, the searching mechanism and the detection mechanism, making and creating the alerts.

“Another valuable aspect is the flow editor, which has helped me a lot in my data analysis. Devo has 400 days of hot storage and you can draw your attack chain from more than a year if you are hunting for threats. The results are very faster because it is working on unstructured data.

“Visualizations in Devo are great. You can create dashboards, and in Devo, we call them active boards. So visualization is very good in Devo. We have created active boards with the LINQ query. It is a similar process like Splunk. In Splunk, you have to write the query for rules, alerts, and dashboards, and in Devo it is the same thing. We create active boards via LINQ query and visualize and select the layout and which layout we want to see the things we want to see on our dashboards. We also utilize this visualization in height and monitoring. For instance, if there are geopolitical tensions between countries and we are monitoring one of the SOCs of those countries, we utilize these dashboards and active boards in height and monitoring..”

Usama Khan

Team Lead Soc at a tech services company with 51-200 employees

[Read full review](#) 

“The data analytics cloud component focuses on real-time analytics, which is very impressive. The SIEM collects and correlates logs data from different sources and can integrate with ServiceNow, hardware asset management, and software asset management. The security orchestration, automation, and response (SOAR) is another valuable feature. The security data platform serves as the foundation of Devo.

“Regarding advanced query capabilities, Devo offers several models including query logs, visual query builder, language integrated query, and SQL, with SQL being the most frequently used querying data capability.

“The single pane of glass that Devo offers is the SOC. The tools in Devo's active ports are for investigating, not just viewing data. They are more interactive than other market solutions. The drill-down reports capabilities allow analysts to click on any element in a widget. When they see a spike in a line chart for a failed login, which could be a true or false attempt, they can click that spike, and a table widget on the same active board instantly populates with raw logs of data for those specific failed logins. This is particularly important for enterprise companies with numerous endpoints and users. The dynamic filtering of inputs significantly reduces the time cybersecurity analysts spend trying to figure out failed logins and identifying false positives..”

Francisco Javier Romo

Strategic Account Executive at a computer software company with 51-200 employees

[Read full review](#) 

One strong feature of Devo is centralized log visibility. Another is fast querying and correlation across multiple data sets. It also supports better investigation because our analysts can quickly search, correlate, and investigate suspicious activity.

In our day-to-day work, fast querying and correlation help reduce our effort because our SOC analysts do not need to manually switch across systems for logs. Correlated visibility helps speed up the investigation and provides more context for decision making. When the analyst uses queries to search, it pulls the data quickly, in a second, which aids us greatly with the investigation.

“Devo helps us improve visibility across different environments and allows better incident tracking. The search and analytics capability is also useful for our teams as well as the security teams.

“Devo has improved our visibility, log management efficiency, and investigation capabilities positively. Teams are able to investigate events with better context and faster access to the relevant data.

“Our analysts can investigate faster when using Devo. It has absolutely reduced our investigation time, improving our investigation quality as well. This helps security teams respond more efficiently.

“Devo's main value comes from improved investigation speed. It has improved significantly, and its centralized visibility has reduced our effort in log analysis. .”

Vikram Chakravarthy

Cyber Security Engineer II (Vulnerability & Threat Management) at FICO

[Read full review](#) 

Other Solutions Considered

Previously, we were using a Securon tool, which is a cloud-based SIEM platform where we did not have much correlation capability. That is the reason we switched to Devo.

Vikram Chakravarthy

Cyber Security Engineer II (Vulnerability & Threat Management) at FICO

[Read full review](#) 

We have evaluated multiple SIEM and analytics solutions before choosing Devo, depending on the scale, integration, and monitoring requirements, including multiple SIEM products and open source options.

Vikram Chakravarthy

Cyber Security Engineer II (Vulnerability & Threat Management) at FICO

[Read full review](#) 

“Previously, we used Microsoft Azure's Microsoft Sentinel, which gathered data but was costly and less user-friendly. When we learned about Devo and its features, UI experience, reporting capabilities, and threat detection automation, we moved to Devo..”

G Srivastava

Senior Cloud Engineer at a tech services company with 201-500 employees

[Read full review](#) 

“I work with Devo. When comparing Devo with Splunk and Carbon Black, I think Devo is the leader.

“I believe this is because it has the updated technology and component..”

Ahmad Zakwan

Principal Consultant at Syntx Sdn Bhd

[Read full review](#) 

“Compared to Fortinet, Devo is easier to use. However, when using ServiceNow, hardware asset management, and software asset management, there is an opportunity to improve on hardware asset management. They simplify the analyst's time to value, particularly in relation to hardware asset management and software asset management, which are very niche markets..”

Francisco JavierRomo

Strategic Account Executive at a computer software company with 51-200 employees

[Read full review](#) 

“Devo stands out for our SOC and NOC teams compared to other tools such as Elastic because of its SIEM capabilities for threat detection and investigation.

“There are other improvements needed when comparing Devo with other tools on the market, especially since we have started using Elasticsearch for DevOps and infrastructure. Elastic is much better and less costly than Devo, and it offers a free tier for first-time use, allowing users to gain a good understanding of the tool. Due to this, we have stopped using Devo in our company for the past six months and have transitioned to Elasticsearch, which is performing well..”

G Srivastava

Senior Cloud Engineer at a tech services company with 201-500 employees

[Read full review](#) 

ROI

Real user quotes about their ROI:

“In terms of return on investment with Devo, I'd say it has been costly due to the need for support and the overtime required for issues experienced at the beginning of the project. I know when we renewed our contract with them, we were supposed to get our own dedicated support, but I don't think that happened. I don't really see those metrics..”

Leland Austin

Senior Consultant and Technical Lead at a financial services firm with 10,001+ employees

[Read full review](#) 

“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..”

Validated user

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

[Read full review](#) 

“Devo gives value to the end user and is saving compared to other products in the same category.

“I think it saves approximately 10 to 15% compared to similar products..”

Ahmad Zakwan

Principal Consultant at Syntx Sdn Bhd

[Read full review](#) 

“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..”

Validated 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](#) 

Use Case

“I have been using Devo as a partner and system integrator for three years. For log monitoring, the clients' use cases can utilize Devo perfectly.

“Compliance and security operation monitoring are the biggest benefits from the product..”

Ahmad Zakwan

Principal Consultant at Syntx Sdn Bhd

[Read full review](#) 

“I am using Devo myself. Basically, I work at an MSSP, and we provide services to the organization for Security Operation Centers. In our Security Operation Center, we provide the service of SIEM via Devo. We also provide the service of SOAR via Devo. We are the vendors of Devo, which is why I have a great experience with it..”

Usama Khan

Team Lead Soc at a tech services company with 51-200 employees

[Read full review](#) 

“During my time at MetaBase Q and as a partner integrator of ServiceNow, I had the chance to understand and be part of projects integrating SOC's, NOCs, and Security Operation Centers with Devo.

“Mostly enterprise customers invest money in security information and event management or security orchestration, automation, and response, such as SOAR or SIEMs.

“Devo integrates with QRadar, Mitre clouds, and Watson..”

Francisco JavierRomo

Strategic Account Executive at a computer software company with 51-200 employees

[Read full review](#) 

“Devo is the bank's centralized log management platform that my team and I rely on the most.

“For centralized log management in our day-to-day work, one of the biggest data users would be our Red Hat Linux, so the RHEL, which is called the box.unix.rhel table. We get a lot of server endpoints, specifically Red Hat Linux, come into Devo, and then we forward that to our SIEM system. When our security teams need to review those logs, they're there, and they can perform queries.

“It depends on what you're looking for, but it's hard to be specific when we do use Devo for a lot of different platforms that send their syslogs to us..”

Leland Austin

Senior Consultant and Technical Lead at a financial services firm with 10,001+ employees

[Read full review](#) 

Devo serves as our centralized log monitoring, threat investigation, alert monitoring, and security analytics platform. We use it to collect logs from multiple systems so we can correlate the events, investigate suspicious activity, and improve our incident management lifecycle and visibility across our organization.

One practical scenario involved investigating suspicious authentication activity where we had to review logs from multiple sources. Devo helped us centralize the data and allowed the team to investigate faster by correlating the logs instead of checking multiple systems separately.

“Devo functions as our centralized visibility and investigation platform, integrated with security workflows. It becomes more valuable when multiple log sources are connected together because it provides a unified SIEM solution.

“Typically, we have integrated Devo into an enterprise monitoring environment, which supports centralized log collection and analytics. .”

Vikram Chakravarthy

Cyber Security Engineer II (Vulnerability & Threat Management) at FICO

[Read full review](#) 

“My main use case for Devo is that it serves as a primary tool for centralized logging solutions, mainly for threat investigation and alert monitoring. It helps us with security and analytic analytics, as we collect all the logs from multiple servers across our three clouds: AWS, GCP, and Microsoft Azure. Devo helps us correlate those events and assists in the investigation of any suspicious activity or improving our incident management lifecycle.

“A specific example of how I use Devo for threat investigation and alert monitoring is that since Devo acts as a centralized logging solution in our company, whenever we face any kind of security alert, such as unauthorized usage of our system or alerts related to threats, we use this tool. This tool provides data in a very fast manner because it utilizes all the data in its raw format. The queries we run in Devo give results quickly, and it integrates well with our ServiceNow tool, so as soon as there is a suspicious activity in our systems, an alert gets generated from ServiceNow..”

G Srivastava

Senior Cloud Engineer at a tech services company with 201-500 employees

[Read full review](#) 

Setup

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

“The initial setup was 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..”

Validated 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..”

Validated 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..”

Validated 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

Security Engineer at Kforce

[Read full review](#) 

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..”

Validated 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

[Read full review](#) 

“I have contacted them a couple of times. They 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

[Read full review](#) 

“The customer service is average. Technical support from Devo is helpful, but they can improve on the support model.

“I think they could improve on the response time..”

Ahmad Zakwan

Principal Consultant at Syntx Sdn Bhd

[Read full review](#) 

The customer experience with Devo has been very good. It depends on the issue, the issue complexity, and the deployment scenario.

I rate the customer support a nine out of ten because of their timely technical guidance and responsiveness during the deployment and troubleshooting periods.
.”

Vikram Chakravarthy

Cyber Security Engineer II (Vulnerability & Threat Management) at FICO

[Read full review](#) 

Other Advice

“Devo has automated machine learning modules that help predict potential threats. The product learns the data and provides additional correlation rules on top of that.

“I gave this review a rating of 8..”

Ahmad Zakwan

Principal Consultant at Syntx Sdn Bhd

[Read full review](#) 

“Regional support in Mexico or Latin America could be improved, as currently almost all support is in English. For account management or partners of ServiceNow or IBM, they have local support, which is an area where Devo could improve.

“On a scale of one to ten, I rate Devo a seven out of ten..”

Francisco JavierRomo

Strategic Account Executive at a computer software company with 51-200 employees

[Read full review](#) 

My advice to others looking into using Devo would be to first understand your logging and visibility requirements. If centralized monitoring and faster investigation are prioritized in your environment, then Devo becomes valuable.

Devo provides a good experience overall. It is an enterprise-grade monitoring platform.

“I would rate this review an eight out of ten. .”

Vikram Chakravarthy

Cyber Security Engineer II (Vulnerability & Threat Management) at FICO

[Read full review](#) 

“I would give Devo a seven out of ten because it has been a good tool, but with the lack of support, it kind of gives me some bias for using the product since it takes a while for issues to get resolved. We are relying on them for enhancements, which is another thing that could take a while to get addressed as well, just based on them being in Spain where their main support team is located, and knowing that they do have other clients as well. Sometimes, as a client, you don't feel prioritized.

“My advice for others looking into using Devo is that it's a good product, but I would reiterate its challenges with support. Devo is a good product with poor support. I rate Devo a seven out of ten..”

Leland Austin

Senior Consultant and Technical Lead at a financial services firm with 10,001+ employees

[Read full review](#) 

“Devo's main job is to provide a centralized logging system, so we do not have to use other logging systems for other servers. It helps us correlate events from our

clouds and third-party clouds, providing all those solutions in one system. Devo is a great tool for anyone to analyze logs and reports.

“Devo helps our teams with incident investigation and security monitoring, and it also assists in providing compliance reports, which helps us improve our systems day by day.

“My advice to others looking into using Devo is that if you have a large or even small customer project and want to utilize SIEM and security threat analytics, you should consider Devo. It is a great tool. However, if you need infrastructure monitoring and DevOps observability, you might want to opt for Elasticsearch. I rate Devo an eight out of ten..”

G Srivastava

Senior Cloud Engineer at a tech services company with 201-500 employees

[Read full review](#) 

“I have majority of experience with Devo and a little bit of experience with Splunk and [LogRhythm](#). I have used its advanced querying capabilities.

“MTTR and MTTD are the most critical metrics for me when using Devo's analytics engine. I utilize the threat link metrics in SOAR for calculating my metrics.

“Devo's automated machine learning models have helped in predicting potential threats, but it needs improvement. It still requires some work because it is not so much vendor agnostic.

“Their SOAR support team is very good, but the SIEM team can do better.

“I would rate Devo around 7.5 out of 10 for technical support. Overall, Devo as a product, I would rate it 9 out of 10.

“I would appreciate seeing more AI automations in Devo and enhancing Security Operation Center's day-to-day tasks. My overall rating for this review is 9 out of 10..”

Usama Khan

Team Lead Soc at a tech services company with 51-200 employees

[Read full review](#) 

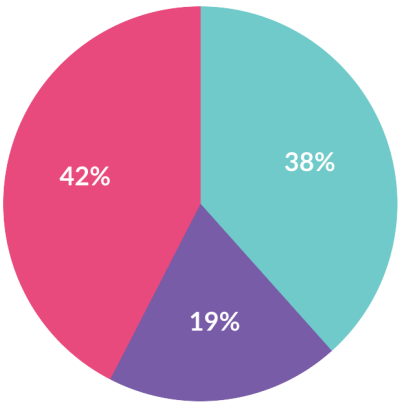
Top Industries

by visitors reading reviews

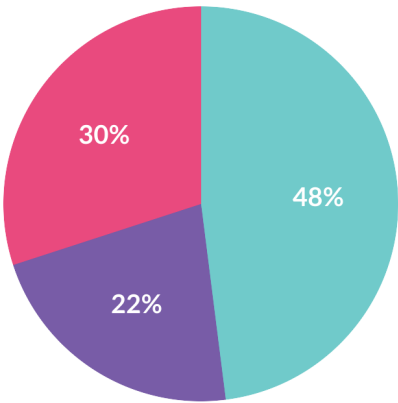


Company Size

by reviewers



by visitors reading reviews



Large Enterprise Midsize Enterprise Small Business

About this buyer's guide

Thanks for downloading this PeerSpot report.

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

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

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

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

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

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

[Get your personalized report here](#)

About PeerSpot

PeerSpot is the leading review site for 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