aws marketplace

IBM Security QRadar

Reviews, tips, and advice from real users






Powered by PeerSpot

Contents

Product Recap

IBM Security QRadar

IBM Security QRadar Recap

IBM Security QRadar offers real-time threat detection, data correlation, and integration with third-party solutions, providing a user-friendly interface, scalability, and extensive reporting capabilities for SIEM needs.

IBM Security QRadar is designed for comprehensive security monitoring in diverse environments, aiding sectors like telecom and finance with advanced threat detection and breach management. It aggregates data and analyzes user behavior, while its customizable and out-of-the-box rules deliver robust security insights and vulnerability management. The platform seeks enhancements in integration, performance, and user interface, with a focus on AI and cloud service compatibility.

What are the most important features of IBM Security QRadar?

- Real-time Threat Detection: Monitors and alerts on security incidents as they happen.
- Data Correlation: Aggregates and connects disparate data sources for cohesive analysis.
- Third-party Integration: Supports seamless interaction with other security tools.
- Scalability: Grows with organizational needs without sacrificing performance.
- Customizable Rules: Allows tailored security settings for specific requirements.

What benefits and ROI should be expected?

- Enhanced Security Insights: Offers comprehensive coverage across environments.
- Reduced False Positives: Minimizes unnecessary alerts, improving efficiency.
- User-friendly Interface: Simplifies navigation and analysis tasks.
- Extensive Reporting Capabilities: Provides detailed insights for informed decision-making.
- Compliance Focus: Assists in meeting regulatory standards effectively.

Telecom, finance, and cloud-based industries implement IBM Security QRadar for threat detection, compliance, and security monitoring. It is deployed for log collection and correlation, user behavior analytics, and ensuring secure data transfer and incident management, focusing on compliance and anomaly detection.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- “The query search and log fetching are really helpful in IBM Security QRadar when compared to other tools.”

HarshBhardiya
SOC Engineer at a outsourcing company with 10,001+ employees

- “I am fond of IBM Security QRadar because it is very user-friendly.”

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

- “The integration of third-party technologies with IBM Security QRadar is one of the high points they have; they integrate with almost anybody, anywhere, and there's an integrator tool for almost anything.”

Mauricio Campiglia
CTO at Sabyk

"IBM Security QRadar's AI and machine learning capabilities for threat detection and response are exceptional, and Q Site is used to create panels and visualizations of software development processes."

Francisco JavierRomo

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

"I suggest others to go with IBM Security QRadar because it is an IBM product and many companies and bank environments are using IBM Security QRadar because of its strong visibility and analysis capabilities."

Abhimanyu Das

Senior Cybersecurity Engineer at Kyndryl

"Currently, it is very stable."

Mahmoud Younes

Cyber Security Architects at VaporVM

"IBM Security QRadar has positively impacted my organization by enabling me to mitigate many incidents and reduce manual tasks by up to 40%."

Verified user

Implementation at a comms service provider with 11-50 employees

What users had to say about valuable features:

“The query search and log fetching are really helpful in IBM Security QRadar when compared to other tools.

Compared to ArcSight, Splunk, or any other SIEM tools where you need their processing language such as structured query language, SPL, and in Sentinel there is KQL query languages, IBM Security QRadar doesn't require reliance on query languages. There are filters which you can use directly and apply to get the data you want fairly easily..”

HarshBhardiya
SOC Engineer at a outsourcing company with 10,001+ employees

Read full review

“IBM Security QRadar has inbuilt components for assessing artificial intelligence and machine learning capabilities that we are currently utilizing.

“I appreciate the technical support provided by the OEM for IBM Security QRadar.

“I have used IBM Security QRadar's analytics for automating SOC tasks.

“The metrics that reflect the benefit of analytics in my case include reporting and user behavior..”

Milind-Kule
Technical Lead at Inspira Enterprise

Read full review

“IBM Security QRadar makes things user-friendly because in the Log Activity tab, you can make a search right away as desired. All filters are available on the tab. You can group logs by source IP, event ID, destination IP, or port. The user interface makes investigation very easy for an analyst.

IBM Security QRadar can work on big data and should start supporting big data as other Gartner's top SIEM products do. An integrated LLM with IBM Security QRadar would be very good for its reputation. I started my career with IBM Security QRadar and totally love it. I do not want it to go down to the bottom of the top 10, but rather be in the top two or three SIEM products in Gartner's rating.

Dashboards are a good feature in IBM Security QRadar, but they can be improved. Other SIEM solutions such as Splunk and LogRhythm are working on integrated LLMs or AI chat..”

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

Read full review

"The best features of IBM Security QRadar, in my experience, include multiple application integrations available through the IBM App Exchange, and I particularly appreciate the Playbook Designer feature, which allows me to design playbooks on a canvas, making it user-friendly and efficient.

"The Playbook Designer in IBM Security QRadar has specifically helped my workflow by allowing the creation of advanced SOAR playbooks, with many sub-playbooks integrated into the main playbook itself. This feature enables me to create great workflows using functions, scripts, and rules tailored to client requirements, and the integration of applications enhances the feasibility of using Playbook Designer while allowing me to expand playbooks as necessary.

"IBM Security QRadar has positively impacted my organization by enabling me to mitigate many incidents and reduce manual tasks by up to 40%. I have noticed a decrease in incident response time and a significant reduction in the number of manual tasks performed, leading to more efficient overall operations.."

Verified user

Implementation at a comms service provider with 11-50 employees

Read full review

"IBM Security QRadar offers a wide range of powerful features. During phishing-related investigations, it greatly assists from an analyst's investigation point of view. A core capability of IBM Security QRadar is visibility — it collects and normalizes logs and network flow events from multiple tools. It can ingest logs from almost any source. Its advanced, modular architecture supports real-time log collection from diverse systems, making it well-suited for environments using platforms such as CrowdStrike, Microsoft Defender, Trend Micro, and Symantec.

These features are highly beneficial in our environment because, from a security perspective, proper log collection and management are crucial. QRadar streamlines SOC operations by automating alert triggers and providing unified visibility across multiple environments, which enhances our team's ability to handle phishing and EDR alerts effectively. The shift handover capability is another valuable feature of IBM Security QRadar. Real-time log normalization and its advanced analytics engine help reduce high-risk alerts and false positives by up to 50%.

From an analyst's perspective, threat hunting and groundwork during rotational shifts, combined with SOAR playbook automation, enable efficient endpoint isolation and quarantine actions. IBM Security QRadar also features a custom rules engine that allows analysts to create dynamic rules using AQL, targeting niche threats such as suspicious domains, all without vendor lock-in. Unlike rigid EDR policies, its petabyte-scale indexing efficiently handles massive event-per-second (EPS) volumes without performance degradation, making it ideal for expanding enterprise environments compared to lighter SIEM solutions.."

Abhimanyu Das
Senior Cybersecurity Engineer at Kyndryl

Read full review

"IBM Security QRadar is a very good SIEM solution because it has features that allow me to create rules or built-in lookups specific to my company. I can tune those to reduce the attack surface and be specific about the right malicious activities to reduce risk about an attack on my company or attacks on endpoints or assets.

IBM Security QRadar offers a good dashboard because it provides many things, including offense, log activity, network flow, reporting, and rules. All of these are very helpful for me as a SOC analyst L1 or a security engineer. I can see networking activities and log activities coming from our clients. IBM Security QRadar gathers information and logs from these sources and determines based on my rules whether to trigger an offense about that rule or not.

IBM Security QRadar is also helpful because when I see any IP or source IP and destination IP, I can search in IBM X-Force to determine if it is malicious or not. I can also scan the IP to see what it is and if it is related to a domain or a suspicious domain. Another very helpful feature is the built-in work or rules created by default from IBM product sales.

IBM Security QRadar has impacted my organization positively by helping me with many things, including catching attacks and moving quickly to reduce damage or risk from attacks. I cannot share specific information about how IBM Security QRadar helped me catch attacks quickly because it is sensitive information about my company, but IBM Security QRadar is helpful and has enabled me to accomplish many things.."

Hamdi Gomaa
Cyber Security (SOC Analyst) at CORELIA

Read full review

Other Solutions Considered

"We chose IBM Security QRadar because we were moving to cloud. Previously it was an on-prem solution. Compared to Splunk and Sentinel, it's much more cost-effective.."

HarshBhardiya
SOC Engineer at a outsourcing company with 10,001+ employees

Read full review

"Yeah, before QRadar, we were piecing things together with a mix of Microsoft Defender for logs from endpoints and some basic syslog forwarding from Trend Micro Deep Security, but it wasn't a full SIEM—just siloed tools that made correlation a nightmare.."

Abhimanyu Das
Senior Cybersecurity Engineer at Kyndryl

Read full review

"We looked at Splunk and Azure Sentinel as main alternatives before landing on QRadar—Splunk for its search power and Sentinel since we're heavy on Azure.."

Abhimanyu Das
Senior Cybersecurity Engineer at Kyndryl

Read full review

"I have been in the cybersecurity field since 2012. I have experience with many cybersecurity products including IBM Security QRadar, Splunk, SOAR, IBM Resilient SOAR, Phantom, and various security controls and products.."

Mahmoud Younes
Cyber Security Architects at VaporVM

Read full review

"Legacy solutions were log management solutions, while IBM Security QRadar is a security information event management SIEM that does all the work which previous multiple solutions were doing separately. IBM Security QRadar does all in one, which mitigated costs. However, I cannot give exact metrics on that because I have not worked on those legacy solutions. I started my career working with IBM Security QRadar SIEM.

I did not switch solutions; I switched companies. My current company had another solution, so I had to work with that because I am not the decision-maker to change the solution of a company. Teams and management are involved in deciding which solution is best for the organization. I can only suggest based on the features of the solution.."

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

Read full review

"We have machine learning for User Behavior Analytics (UBA), but IBM Security QRadar does not have AI connectors or integration with ChatGPT. Some SOARs are working with AI, such as FortiSOAR, which has chatbot and AI integration with ChatGPT to create playbooks, assist analysts in exporting reports, and provide recommendations for alert responses.."

Mahmoud Younes
Cyber Security Architects at VaporVM

Read full review

ROI

Real user quotes about their ROI:

"Most of our clients have seen a return on investment because compared to other solutions it does not require a busload of people to operate it and it is reasonably priced.."

James Riffenburg
Principal Cybersecurity Consultant (Architecture, Engineering, Operations)
CISO VCISO at a financial services firm with 10,001+ employees

Read full review

"I have not calculated ROI for this product. QRadar UBA is a tiny part of the entire security portfolio. In the context of the SIEM as a whole, the cost is so low that it's hard to defend not doing it.."

Kjell Morkeng
Head of Cyber security analysis at DNV Poland Sp. z o.o.

Read full review

“The tool's ability to redeploy resources, like manpower, is about the same as that of other competitors. The benefit the tool offers is the protection and the ability to act on whatever the situation might be quickly, efficiently and terminate whatever is happening. The tool is useful to the bottom and helps with the remediation part..”

Verified user

Executive Vice President at a computer software company with 11-50 employees

Read full review

“Implementing IBM QRadar is similar to investing in insurance for our organization's security. While the return on investment may not be immediately tangible, it is crucial for mitigating potential disasters and ensuring our organization's resilience against security threats in the long run..”

MUHAMMADNADEEM1

Deputy Director at Board Of Revenue

Read full review

"In terms of return on investment, I have worked on exercises where the payback occurs within three or four months, which is very good for a cloud solution because implementation cycles can be really long. AWS gives the chance to implement a solution out of the box with use cases that are already in IBM Security QRadar. Solutions such as Q Business, Q Site, QuickSight are already out of the box, so implementing and configuring a use case takes about two to three months, with the payback being almost immediate.."

Francisco JavierRomo

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

Read full review

"ROI calculation is more applicable when using SOAR rather than SIM. In SIM, you don't have functions or enrichment to check if an IP is malicious or different reputations or websites. With SOAR, you can calculate ROI. For example, when an analyst receives alerts on IBM Security QRadar Offense, they would typically take 10 to 15 minutes to check an IP in VirusTotal, AbuseIPDB, TotalVirus, and other sources. With SOAR, the workflow takes one minute or less to complete the analysis.."

Mahmoud Younes

Cyber Security Architects at VaporVM

Read full review

Use Case

"The use cases are daily monitoring, asset management, asset monitoring, asset health status monitoring, and alert monitoring. That is the current use case of what SIEM is being used for.."

HarshBhardiya
SOC Engineer at a outsourcing company with 10,001+ employees

Read full review

"I am currently a consultant specializing in cybersecurity solutions rather than software. IBM Security QRadar is the SIEM platform that I am working with.."

Milind-Kule
Technical Lead at Inspira Enterprise

Read full review

"I use IBM Security QRadar to collect logs, analyze them, and share details. When I began investigating incidents and working with the SOC team, I was using IBM Security QRadar.."

Abhimanyu Das
Senior Cybersecurity Engineer at Kyndryl

Read full review

"My main use case for IBM Security QRadar is its good features which create an offense or trigger an offense. This offense has a description and contains many events with sensitive or helpful information about the offense. My daily activity as a SOC analyst L1 is to ensure if the offense is legitimate, if it is truly a suspicious or malicious offense, or a false positive. After that, I create a ticket to close it and determine if it is suspicious or not. If I need to conduct more investigation and delegate the ticket further, I escalate it to SOC L2 or the SOC Manager to take additional activities or conduct more investigation about it.."

Hamdi Gomaa
Cyber Security (SOC Analyst) at CORELIA

Read full review

"I was a SIEM administrator using IBM Security QRadar for ingesting log sources from all over the digital infrastructure of the organization I worked for. After ingesting logs from all servers and applications, I used the use case manager and offenses.

I managed and handled several incidents in IBM Security QRadar by creating many rules. I created a rule for Dark Web communication from the internal network of the organization. Based on that, I created a rule named Anonymous Tor Connection in which I called the reference set from the reference set type that I created for blacklisted IPs of Tor nodes and called it in the rules. If any of those IPs were detected as the destination IP from an internal network source IP, the alerts would trigger.

I created brute-force attack rules based on Windows Event IDs and created more rules for failed login attempts and audit success.."

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

Read full review

"IBM Security QRadar is primarily used for orchestration, automation, and incident response in my environment.

"I use IBM Security QRadar for automation and incident response through a phishing mail playbook, where an employee sends a malicious phishing email to the SOAR inbox, and SOAR automatically generates an incident based on that email. After the incident is generated, we have created an advanced playbook that analyzes and scans the incident artifacts, extracting malicious elements in the notes. Following the identification of malicious content, another playbook sends an email notification about the findings and integrates with firewalls to automatically block the IOCs identified in the email. This is one of several playbooks we have developed.

"Regarding my main use case for IBM Security QRadar, I have used most of IBM Security QRadar by integrating it with IBM Security QRadar SIEM, consolidating many IBM Security QRadar SIEM alerts in IBM Security QRadar SOAR. We have created incident types for each IBM Security QRadar alert and handle each incident carefully in IBM Security QRadar SOAR, automating incidents at an advanced level, including the use of a custom SOAR SDK to develop a custom SOAR application to meet client requirements. We have leveraged the potential of IBM Security QRadar SOAR.."

Verified user

Implementation at a comms service provider with 11-50 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.

"For the initial setup of IBM Security QRadar, you need to have the right people, but if you are a newbie to these kinds of solutions and want to do out-of-the-box implementations, Amazon provides out-of-the-box use cases that you can implement immediately, and the personalization is easy to accomplish.."

Francisco JavierRomo

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

Read full review

"Setting up IBM Security QRadar is difficult; it has a deep learning curve for the analysts, and there are several hurdles to handle to get IBM Security QRadar running on your infrastructures. On the other hand, once you connect the dots, they keep sending the information, and you can continue getting those events.."

Mauricio Campiglia

CTO at Sabyk

Read full review

“Deploying IBM Security QRadar was quite simple for me, and I was able to complete it by myself without any help.

“It did not take much time for me to deploy it; it took one week. The week it took was for configuration and onboarding, as it is a complete solution and not only an installation..”

Milind-Kule

Technical Lead at Inspira Enterprise

Read full review

“On a scale of one to ten, if ten means easy, I rate the product's initial setup phase as an eight.

As long as you have your policies and if they all relate to security and other areas like infrastructure, then the rules are pretty easy to feed into the product.

The time needed for the product's deployment phase depends on how the entity, the client, has its policies and rules set up. I don't want to say the tool is like a plug and play product because nothing really is in today's market. The tool offers ease of use and integration. I rate the tool a seven to eight for the ease of use and integration it offers..”

Verified user

Executive Vice President at a computer software company with 11-50 employees

Read full review

“We didn't face any difficulty in the deployment process. The strategy we follow in the deployment is a phased approach. Initially, we deployed the workspace, and then we moved to routers and hardware-related things. In phase two, we start integrating the tool with business applications.

The solution is deployed on an on-premises version.

The solution can be installed for the initial configuration and settings in around three to four hours or five hours. Asset onboarding varies. Through assets, we integrate very quickly, like switches and data, with instances where no approval is required. Other typical assets like this are applications where certain views we have to create certain views in order to create our fetch logs. It all depends from application to application.

Three or four people are required to install the tool. Actually, we have a team and deployed the tool with five people. Two people did installations, and two people are supporting, and getting the required things or approvals would be done. You can say it is normally a team of five engineers. They actually take part in maintenance, too. Actually, we divided it into two phases, like team deployment and implementation. One has a team of engineers with whom we are involved with the deployment and installation. Another is the SOC team, which is responsible for monitoring logs on IBM Security QRadar..”

Muhammad Misbah

RETAIL BANKING AND AML/KYC MANAGER at National Bank of Pakistan

Read full review

“The initial setup is user-friendly and straightforward, making deployment easy. However, compatibility issues with other security controls still need to be addressed. It provides a 35-day period for project enablement. This timeframe is too short and should be extended to 45 or 50 days.

When deploying QRadar on-premises, we assess the organization's size to determine the required number of UPS units, application servers, and other necessary hardware. Once these requirements are identified, we proceed with the deployment.

We face challenges in the deployment phase, especially when working with an MSSP license. The main issue is with QRadar's multi-tenancy, which often causes the system to crash. Their support services are not very helpful in addressing these problems.

We allocate two working days for the deployment of QRadar for our customers. Our team includes a senior engineer who communicates with the client and a junior engineer responsible for deploying and installing other services.

The deployment time can vary based on the size of the setup. Large deployments, such as those with 20,000 to 25,000 EPS for corporate clients, take longer due to the need for multiple hardware servers. In such cases, it can take several days. QRadar can be installed in about three to four hours for smaller setups..”

Maaz Khalid

Manager SOC at Rewterz

Read full review

Customer Service and Support

"Our partners in Turkey support QRadar integration because our team does not manage all aspects. We usually rely on local partners for support. They assist with advanced issues, such as hardware or other problems, that are not part of standard operations.."

VuralSanal
Network and Security Architect at Deutsche Telekom

Read full review

"I would rate their support an 8.5 with IBM. The support is really good; for instance, if a critical ticket is submitted, you will get paged right away as it gets logged, and their analyst will look into it, letting you know as soon as possible so you can work on it. If there is something bad going on or something faulty with IBM Security QRadar, when you reach out to them, they reply in 10 to 20 minutes.."

Jwal Patel
Cyber Security Intern at a retailer with 1,001-5,000 employees

Read full review

"When I upgraded IBM Security QRadar to version 7.4.3, my log sources disappeared after upgrading to the next version. I opened a support ticket and the team told me that this version had a bug. They instructed me to go into the user account and change the language to US English or Canadian English. After I did that, I obtained all the log sources back. This was a really troubling bug in IBM Security QRadar, as it is a world-class product but has that type of bug. Customer support and scalability were very fine.."

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

Read full review

"The customer service experience is mixed. For critical issues, they provide L1 support rather than expert support initially. The L1 support follows standard steps before escalating to the development team or expertise team. In critical situations, this process can be problematic. Support needs to understand the issue first, then escalate it to the engineering team. The engineering team then sends an appointment meeting about the issue. This process can result in outages lasting three to four hours.."

Mahmoud Younes
Cyber Security Architects at VaporVM

Read full review

"I would rate their customer service or technical support as the best in Mexico. The only issue is the language barrier sometimes, because customer support services are used from India, and that can be challenging. While I speak English, it's difficult to understand some accents. However, besides that, local support in Mexico has people ready to provide level one, level two, and level three support. When something complex arises, the ticket gets transferred to India or to third parties not in Mexico, but it's very difficult to scale a ticket that far. The customer support located in Mexico speaks Spanish and they help to resolve issues, depending on the agent.."

Francisco JavierRomo

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

Read full review

"I find IBM support to be nice. However, as a former IBMer, I may have had some advantages in getting support because I had some contacts. The support information is correct; you get to the information and access the technical documents you need because the information is there, and they used to care about their product. I don't know how it's going to be once the program is fully under Palo Alto's management.

"For the support team, I would rate IBM support an eight, a solid eight. With the support we used to have within IBM, it was good.."

Mauricio Campiglia

CTO at Sabyk

Read full review

Other Advice

"We do not have any use case for easily integrating with third-party tools like Microsoft or AWS. IBM Security QRadar is the only vendor I am using. I rate this product seven out of ten.."

Milind-Kule
Technical Lead at Inspira Enterprise

Read full review

"My advice is that IBM Security QRadar is good. Splunk is also good, but IBM Security QRadar has many features including rules by default that I can tune the speed of. The core advice is that every SIEM is good, but what you will do with them and what you will work on with them is the secret. I would rate this product a 9 out of 10.."

Hamdi Gomaa
Cyber Security (SOC Analyst) at CORELIA

Read full review

"For others looking into using IBM Security QRadar, my advice is to first learn IBM Security QRadar SOAR. Training is essential, but IBM Security QRadar SOAR is not overly complicated, and the documentation from IBM's portal is quite good. By learning IBM Security QRadar SOAR first, users can operate it more efficiently and leverage its versatile features, including rules, workflows, and various custom properties. I would rate IBM Security QRadar a score of six out of ten.."

Verified user
Implementation at a comms service provider with 11-50 employees

Read full review

"I recommend IBM Security QRadar because it is a trusted IBM product that many organizations and financial institutions use for its strong visibility and analytical capabilities. I have had a great experience working with IBM Security QRadar. From what I know, most SOC professionals agree that once you gain experience with QRadar, adapting to any other SIEM tool becomes much easier. Overall, I would rate my experience with IBM Security QRadar highly due to its robust features and wide industry adoption.."

Abhimanyu Das
Senior Cybersecurity Engineer at Kyndryl

Read full review

"IBM Security QRadar is capable of handling much of the market requirements. It's comparable to any other SIEM tool without standing out significantly.

It's fairly open for custom integrations, but it depends on what type of logs we are receiving and what kind of parsing we are getting done. The integrations are totally based on the skill sets if third-party or custom integrations are required.

When it comes to log management, it's fairly easy to manage and the log rotate is really good compared to any standard SIEM tool. It just gets the work done.

I rate IBM Security QRadar an 8 out of 10.."

HarshBhardiya
SOC Engineer at a outsourcing company with 10,001+ employees

Read full review

"Dark theme and white theme are enabled in the latest version of IBM Security QRadar, which is great. An integrated LLM such as Watson should be included in which I can enter an IP address and perform threat hunting steps on it. IBM Security QRadar should tell me what the possibilities of threats are on the specific source IP that I provided. Unstructured data should be supported as Elastic and Splunk work on big data, so IBM Security QRadar should start doing that too.

My day-to-day tasks were to check if the nightly backup is being created, whether there are any undeployed changes in IBM Security QRadar, and to check for new vulnerabilities in my current version to ensure my version is stable and all nodes are working properly. I verify that the HA component of my QRadar's console event processor is synchronized properly and that the data node is balancing all data between the nodes of IBM Security QRadar. If any integration comes up on my desk, I work on the integrations, and if any log sources are in error, I troubleshoot them whether they are database, Linux, Windows, or custom log sources.

I am fond of IBM Security QRadar because it is very user-friendly. I gave this review a rating of 7.5 out of 10.."

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

Read full review

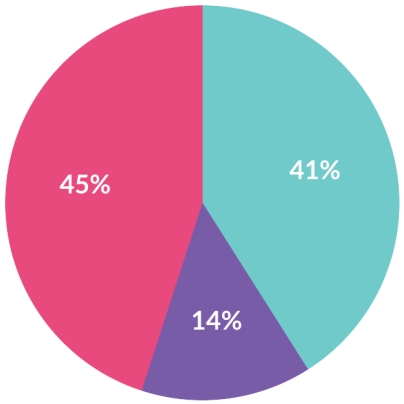
Top Industries

by visitors reading reviews

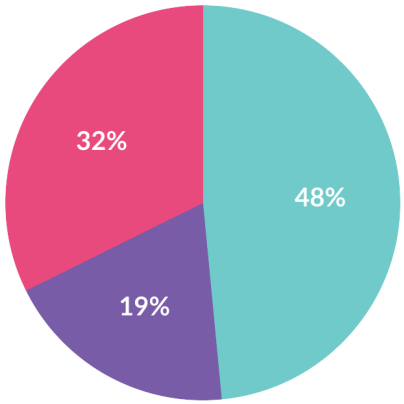
Outsourcing Company	12%
Financial Services Firm	10%
Construction Company	9%
Manufacturing Company	8%

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