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 (recently acquired by Palo Alto Networks) is a security and analytics platform designed to defend against threats and scale security operations. This is done through integrated visibility, investigation, detection, and response. QRadar empowers security groups with actionable insights into high-priority threats by providing visibility into enterprise security data. Through centralized visibility, security teams and analysts can determine their security stance, which areas pose a potential threat, and which areas are critical. This will help streamline workflows by eliminating the need to pivot between tools.

IBM Security QRadar is built to address a wide range of security issues and can be easily scaled with minimal customization effort required. As data is ingested, QRadar administers automated, real-time security intelligence to swiftly and precisely discover and prioritize threats. The platform will issue alerts with actionable, rich context into developing threats. Security teams and analysts can then rapidly respond to minimize the attackers' strike. The solution will provide a complete view of activity in both cloud-based and on-premise environments as a large amount of data is ingested throughout the enterprise. Additionally, QRadar’s anomaly detection intelligence enables security teams to identify any user behavior changes that could be indicators of potential threats.

IBM QRadar Log Manager

To better help organizations protect themselves against potential security threats, attacks, and breaches, IBM QRadar Log Manager gathers, analyzes, preserves, and reports on security log events using QRadar Sense Analytics. All operating systems and applications, servers, devices, and applications are converted into searchable and actionable intelligent data. QRadar Log Manager then helps organizations meet compliance reporting and monitoring requirements, which can be further upgraded to QRadar SIEM for a more superior level of threat protection.

Some of QRadar Log Manager’s key features include:

- Data processing and capture on any security event
- Disaster recovery options and high availability
- Scalability for large enterprises
- SoftLayer cloud installation capability
- Advanced threat protection

Reviews from Real Users

IBM Security QRadar is a solution of choice among users because it provides a complete solution for security teams by integrating network analysis, log management, user behavior analytics, threat intelligence, and AI-powered investigations into a single solution. Users particularly like having a single window into their network and its ability to be used for larger enterprises.

Simon T., a cyber security services operations manager at an aerospace/defense firm, notes, "The most valuable thing about QRadar is that you have a single window into your network, SIEM, network flows, and risk management of your assets. If you use Splunk, for instance, then you still need a full packet capture solution, whereas the full packet capture solution is integrated within QRadar. Its application ecosystem makes it very powerful in terms of doing analysis."

A management executive at a security firm says, "What we like about QRadar and the models that IBM has, is it can go from a small-to-medium enterprise to a larger organization, and it gives you the same value."

Valuable Features

Excerpts from real customer reviews on PeerSpot:

✓ “Currently, it is very stable.”

Mahmoud Younes

CyberSecurity Architects at VaporVM

✓ “The dashboard is easy to use and easy to understand what's going on and what the alerts mean.”

Md. Shahriar Hussain

Information Security Analyst at Banglalink

✓ “My overall rating for this solution is nine out of ten.”

VuralSanal

Network and Security Architect at Deutsche Telekom

✓ “Regarding the tool's ability to maintain high-security standards, I rate it ten out of ten.”

Muhammad Misbah

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

✓ “I think QRadar is stable and currently satisfies my needs.”

JanHoužvička

Architect of Cybersecurity at ASSIST - Software Services

✓ “The most valuable feature of the solution is its ability to rectify a situation involving any anomalies expeditiously.”

Verified user

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

✓ “think QRadar is great overall. We’ve had a positive experience with it and recommend it for deployment. However, there are areas for improvement. The technical support is good, and the documentation is valuable, but it could be enhanced, especially regarding integration with other systems.In terms of support and updates, QRadar’s capabilities are crucial for maintaining high security standards. Network and software administrators can monitor all traffic effectively, which reassures clients and drives further adoption.”

Muluken Mekonene

Network Engineer at Insa

What users had to say about valuable features:

IBM Security QRadar had good rulesets, and the scenarios we could write regarding the compliance-related issues were quite helpful. We mostly used it for prevention.

Verified user

Sales Manager at a financial services firm with 10,001+ employees

Read full review

“The best aspect of Pareto is its user-friendliness. Unlike other solutions requiring query language knowledge, Pareto is entirely GUI-based. This makes it easy to use and understand without learning any query languages..”

Maaz Khalid

Manager SOC at Rewterz

Read full review

“I use standard rules and special user-defined or correlation rules. I also use behavioral analysis for users. Additionally, there is limited integration with other systems. IBM is seeking information about IBM QRadar because a part of QRadar, especially in the cloud, has been sold to Palo Alto..”

JanHoužvička

Architect of Cybersecurity at ASSIST - Software Services

Read full review

“Actually, the dashboard is very good. The dashboard is easy to use and easy to understand what's going on and what the alerts mean. It's very user-friendly, I would say. So far, it's very good. Recently, I faced an incident, a cyber incident, and it was detected in real time. It correlates well with other solutions. I have EDR, vulnerability, and IPS, and it shows useful findings for root cause analysis..”

Md. Shahriar Hussain
Information Security Analyst at Banglalink

Read full review

“IBM Security QRadar is stable. The tool exhibits minimal vulnerabilities and does not encounter multiple issues. It is not easy to operate, it ensures minimal downtime. Its usability, synchronization with systems, user interface, and storage capabilities are crucial. Storage is essential for research and hunting, as it involves delving into logs. The response time of IBM QRadar is commendable, and even when processing large amounts of data, it maintains a consistently high level of performance. The tool utilise RAM efficiently..”

SaiKrishna2
Cyber Security Analyst at Diyar United Company

Read full review

“The aggregations are valuable when creating use cases with aggregations, which is beneficial for us.

“For automation, we are using multi-platform solutions. We have FortiSOAR and IBM Resilient for IBM Security QRadar orchestration. We integrate with both IBM Security QRadar and ArcSight, as we are working with customers who use both systems..”

Mahmoud Younes
CyberSecurity Architects at VaporVM

Read full review

Other Solutions Considered

“The main difference between Splunk and IBM is that the former one is on the edge in terms of innovation, but the latter one is not that good. Compared to IBM Security QRadar, IBM X-Force is good..”

Verified user

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

Read full review

“After going through the different reviews over the internet, we found out that IBM is a leader, and we also did a study of the various banks in Pakistan and internationally to find what products they use. After comparing these banks, international banks, and locally made products, we decided to go for IBM..”

Muhammad Misbah

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

Read full review

“My company is looking for different products in the market since we are upset with the recent news about the deal between IBM and Palo Alto. I think the deal doesn't touch the on-premises IBM Security QRadar, and both companies have only agreed to give Palo Alto the authorization for the cloud version, making it a reason why we continue to use the on-premises version..”

Dmytro Petrashchuk
CTO at IT Specialist LLC

Read full review

“Previously, I had another SIM before IBM brought it up, but I couldn't correlate with different solutions. Now it saves me at least one hour, sometimes up to three hours. I used Micro Focus, which I think was acquired by another company, possibly OpenText. The ownership changed. I am very satisfied with Qradar compared to OpenText. It's superior. I am not sure which one is best, but so far it is. My people had good training and needed to invest time to get good results..”

Md. Shahriar Hussain
Information Security Analyst at Banglalink

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
CyberSecurity Architects at VaporVM

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
CyberSecurity 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

“There are an abundance of customers in the market who are actually using QRadar for their security monitoring purposes. This is a real advantage of this solution..”

Verified user

Senior Security Architect at a tech services company 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

“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
CyberSecurity Architects at VaporVM

Read full review

Use Case

“I use it daily because it's shared as a log alert, and we have a security operations center. Every now and then, and almost every day, there are some alerts. I utilize it every day, twenty-four by seven, as you can see..”

Md. Shahriar Hussain
Information Security Analyst at Banglalink

Read full review

“Basically, it is a product that serves as an SIEM solution, and its main competitor is Splunk. Splunk and IBM are lookalike tools. IBM Security QRadar hosts a panel where you can feed just about anything you can think of in terms of electronics as it relates to security, along with other elements of infrastructure. The tool provides notification of events..”

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

Read full review

“Most of the use cases are based on MITRE ATT&CK, such as phishing email, DDoS attack, privilege escalation, all MITRE ATT&CKs with scanning the environments, using suspicious activity internal to our network. We have thousands of use cases covering different domains at network levels.

“We have use cases covering security controls and firewalls. We also have use cases that cover Active Directory, server events, and Citrix. Because we are working in a telecom company, we are covering 5G and 4G logs..”

Mahmoud Younes

CyberSecurity Architects at VaporVM

Read full review

“We use IBM Security QRadar for storage. These tools are setting high tools on the usage of the logs from multiple devices. It manages millions of logs from multiple devices, such as firewalls, routers, switches, etc. The solution is stable and has better support than LogRhythm. It doesn't have multiple components or servers, troubleshooting, or remote servers. It is based on a CentOS platform, and implementation is difficult..”

SaiKrishna2

Cyber Security Analyst at Diyar United Company

Read full review

“I’m working with the on-prem version of IBM Security QRadar. We initially deployed it with the help of IBM’s professional services for a client, but now we handle deployments ourselves. The process is quite straightforward for us because we gained knowledge from our first implementation and used the available documentation. Deployment takes a couple of hours the first time, including configuration and integration with third-party devices. I usually work with a colleague, so two people handle the deployment. Our environment is well-suited for this, and we’re using it on a virtual appliance. The experience has been smooth and efficient.

We are promoting QRadar to various financial institutions, including banks and microfinances, as a superior option compared to other vendors like Fortinet. While some institutions are using other solutions, we are encouraging them to switch to QRadar for better security.

.”

Muluken Mekonene
Network Engineer at Insa

Read full review

“I have experience with Centimeters solutions, one of which is Microsoft Sentinel. I often confuse the names, but I mean Sentinel. I also have experience with QRadar. In the past, I worked with Elasticsearch. I have generally configured some integrations, for example, between QRadar and other production environments for sending custom logs, though not all of them. I have been doing this for about two to three years. Usually, devices do not send CF in syslog or CS format logs, so we often troubleshoot on a Vural collector. Sometimes a device does not send the packet to a local collector, and we troubleshoot from the local collector's side. My colleagues and I generally use this management for production. I have integrated some network and security devices to send logs. In Turkey, there are regulations by the government that require collecting Internet traffic from VDS users. We need encryption on each log on QRadar. I focus on setting up this configuration. Our customers use Cisco StealthWatch, formerly known as NDR solutions, and we integrated these logs with QRadar and StealthWatch because we prefer not using all of them on NDR solutions. We send specific logs from StealthWatch. This integration is basic, not advanced, though there are some easy API integrations for communication between devices..”

VuralSanal
Network and Security Architect at Deutsche Telekom

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.

"Our experience with the initial setup of QRadar was smooth because we opted for a managed security solution through our service providers. The installation itself took about one to two hours but integrating various sources, creating use cases, fine-tuning, and enabling logs could take up to two to three months. However, in our enterprise network deployment, we managed to accomplish it within six months.."

MUHAMMADNADEEM1

Deputy Director at Board Of Revenue

Read full review

“The number of log sources significantly impacts deployment complexity. The process becomes more complicated for environments with 50 log sources compared to those with fewer sources (e.g., 20 or 10).

Each log source requires a connection to IBM, a task that can take several days or hours, depending on its complexity.

On average, the entire deployment process spans six to eight weeks..”

Ayoub Jaaouani

Solutions Architectv at Smarttech247

Read full review

“The initial setup is straightforward and can be done within a day. It is based on Linux. If there is any issue, you need to bang your head to solve the issue.

IBM Security QRadar requires a specific server with a minimum of 128 GB RAM and can support up to 2,000 endpoints. The installation process involves obtaining the ISO and setting up the necessary configurations. Once installed, we must ensure the components are properly located and configured.

One person is required for maintenance and deployment each.

I rate the solution's setup as a seven out of ten..”

SaiKrishna2

Cyber Security Analyst at Diyar United Company

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

"I am unsure because the problem escalates through level one to level three, and then the process starts over with Novo again. This is problematic for technical support.."

JanHoužvička
Architect of Cybersecurity at ASSIST - Software Services

Read full review

"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

“Troubleshooting delays have been a recurring challenge. Occasionally, responses take two to three days, leading to escalations. While their website’s knowledge base is commendable, troubleshooting scenarios demand more time. My observation is that they may be understaffed..”

Ayoub Jaaouani

Solutions Architectv at Smarttech247

Read full review

“The solution's technical support is responsive. The only area where I don't agree with IBM Security QRadar's technical support stems from the lack of proper or defined recovery time, even though their response time is good.

I rate the technical support a seven out of ten..”

Verified user

Head of Cybersecurity at a computer software company with 51-200 employees

Read full review

“The solution's technical support works, but sometimes, it can take quite a long time to get a solution from technical support. Generally, we are satisfied because we just understand how it works and that you shouldn't expect much from the technical support. It is not so bad, but sometimes it could be longer than you can expect. I rate the technical support a six to seven out of ten..”

Dmytro Petrashchuk

CTO at IT Specialist LLC

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
CyberSecurity Architects at VaporVM

Read full review

Other Advice

“In the middle of evaluating, I am looking for some information about comparison boxes or licenses, products, and so on. I am interested in this issue, but I will not purchase it personally. We have a plan for internal projects for this. Product rating: five out of ten..”

JanHoužvička
Architect of Cybersecurity at ASSIST - Software Services

Read full review

“All technologies are advancing towards AI integration. It is essential to integrate AI capabilities into devices to keep pace with future technologies and integrations. We should configure AI technologies in these products, though we currently lack experience and information. My overall rating for this solution is nine out of ten..”

VuralSanal
Network and Security Architect at Deutsche Telekom

Read full review

“This implementation process receives a rating of six. In UAE, we have strict restrictions regarding compliance, particularly NIST compliance. Most companies should have local LLM, not public. Most SIM solutions or SOAR don't have the capability to build or need custom connectors for using AI with internal LLM, rather than cloud-based solutions ChatGPT or Gemini. Overall, I would rate IBM Security QRadar an eight out of ten..”

Mahmoud Younes
CyberSecurity Architects at VaporVM

Read full review

“My advice is to understand your infrastructure first. Assess the size before sending any protocol requests or RFPs to adjust licensing costs. You may procure licenses less or more than needed, impacting finances. Analyzing your infrastructure is crucial, considering the logs and security issues you will set. Trained personnel are necessary. Without them, usage is challenging. Overall, the product rating is eight out of ten..”

Md. Shahriar Hussain
Information Security Analyst at Banglalink

Read full review

“QRadar offers a clean solution with straightforward integration for various devices. Once you define your scope, you effectively gain visibility into it. When comparing QRadar to other SIEM solutions like GloD and Splunk, QRadar lags behind other modern advancements. While new SIEM solutions focus on data lakes and big data, QRadar continues to rely on traditional correlation modules.

QRadar should prioritize R&D and product improvement. Their support services have also declined and need attention.

In QRadar's user behavior analytics, we observed an alert triggered by an unusual login attempt from one of our administrators. While monitoring alerts during my shift, QRadar's anomaly-based detection identified a login attempt outside normal hours. The system detected this as a deviation from the established baseline since the administrator had never logged in at that time before. This triggered the alert, helping us identify the compromised account.

QRadar requires ongoing maintenance, and running it effectively often depends on support from engineers. Unlike big data tools, QRadar can struggle with integration and may require fine-tuning, restarts, or troubleshooting if issues arise. Since its merger with other companies, we've encountered many problems and have experienced delays in receiving timely technical support.

You don’t need to learn any additional tools to use the system. It allows you to create dashboards from a management perspective, and its user behavior analytics work very well, although the AI analytics module is still developing.

When handling compliance requests or forensic investigations, an SIEM solution like QRadar is essential. It helps pull up logs and identify what happened during incidents or breaches.

The time required for investigation depends entirely on the impact of the attack. Sometimes, only a single device or network is compromised, which may be resolved quickly. However, the investigation takes longer in cases where the scope is broader, involving multiple devices and networks. The timeframe is driven by the extent of the incident, not just by QRadar.

QRadar is a good product. In Pakistan, many financial sectors are starting to shift towards other solutions. In South Asia, particularly Pakistan, has a growing trend towards Splunk. Similarly, there is a shift towards Splunk, LogRhythm, and RSA in the Gulf region.

Overall, I rate the solution a seven out of ten..”

Maaz Khalid
Manager SOC at Rewterz

Read full review

“Speaking of how the tool handles real-time threat management in our specific industry, I would say that for our company's services, which are used with Crows Nest Software, we face the product as per the policies and rules that are set up within an entity or a client. For instance, if we see an anomaly, like if I send you an email, and we are within the same company, or I am within this ABC company, and you are external to it. If I am sending you information that I am not allowed to send outside of the company, what happens is we can either stop it ourselves, especially if that is what the instructions are through the policy, or if the client says, then we send such information to IBM Security QRadar and as per the instructions and policy, they can terminate it or do what they will with it after it is terminated.

Speaking about how anomaly detection has impacted security operations, if I consider it from a dollars and cents point of view, I would say that if I am sending you something that is intellectual property and they stop it, it is like you can put a price tag on it after it is leaked, but prior to it, things could seem hard. For instance, if I am a nefarious individual in a company, then in most cases, I would be sending information outside of the organization to somebody who is in the government or serves as a contractor of a nation or a state. They can then take such information and build whatever they want as far as the competition is concerned and be in the competitive marketplace with my product. Such instances happen all the time with government contractors. When I say government contractors, they are those who deal in military hardware development, and, for that matter, they may be involved in a business revolving around air conditioners. In the market concerning air conditioners, there might be someone who has perfected a new way of pulling moisture out of the air and making it into ice cream, which may seem ridiculous.

In the tool, the rules are really external. The good rules are external, and when I say that, it means it goes with the development of your security policies or your policies in general as they relate to security. When sitting down with the client, to be honest, what happens is that if they are installing something like this and they are developing rules and policies to go with it, it acts as an eye-opener for a lot of folks. With some companies, we classify data according to what we are able to pull. Suppose it is data that we have been given access to. In that case, we can determine and produce how it is in a snapshot over a two-week period and sit down with a client or somebody like a consultant firm to help in the area of BPM or something that can be like a spin-off of KPMG, and they do an excellent job of working with us. To prepare policies and rules, and those can be easily, you know, migrated or installed into any product, like Splunk and IBM Security QRadar.

IBM offers Watson for machine learning and artificial intelligence. I feel IBM has done a pretty good job with it.

We have partnered with various groups and companies that enhance their products, and we are continuing to do that. Since we utilize machine learning and AI from the start, we are well-versed in both areas. Additionally, we are working on something innovative with blockchain, as well as collaborating with another company focused on classification. There are companies on the periphery that specialize in the classification of various things, and they do tasks we don't handle on the front end. They provide us with information, and we share it, enabling us to interface more effectively with platforms like Splunk, QRadar, or others.

I rate the tool an eight out of ten.."

Verified user

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

Read full review

Top Industries

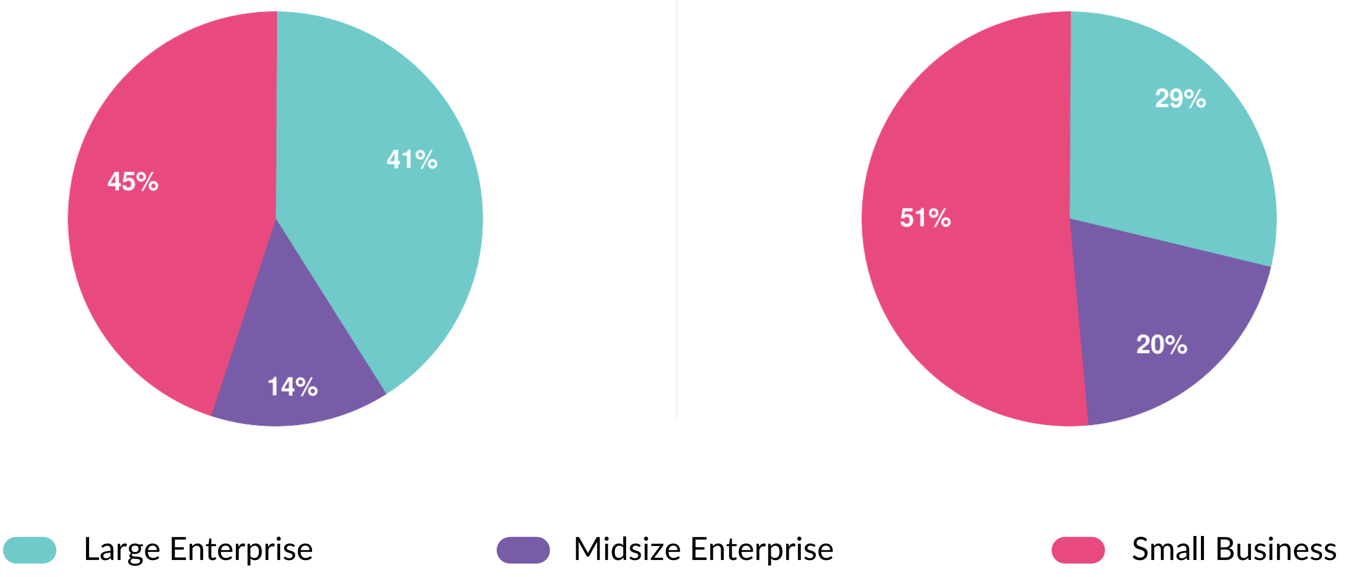
by visitors reading reviews

Computer Software Company	16%
Financial Services Firm	11%
Manufacturing Company	7%
Government	7%

Company Size

by reviewers

by visitors reading reviews



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