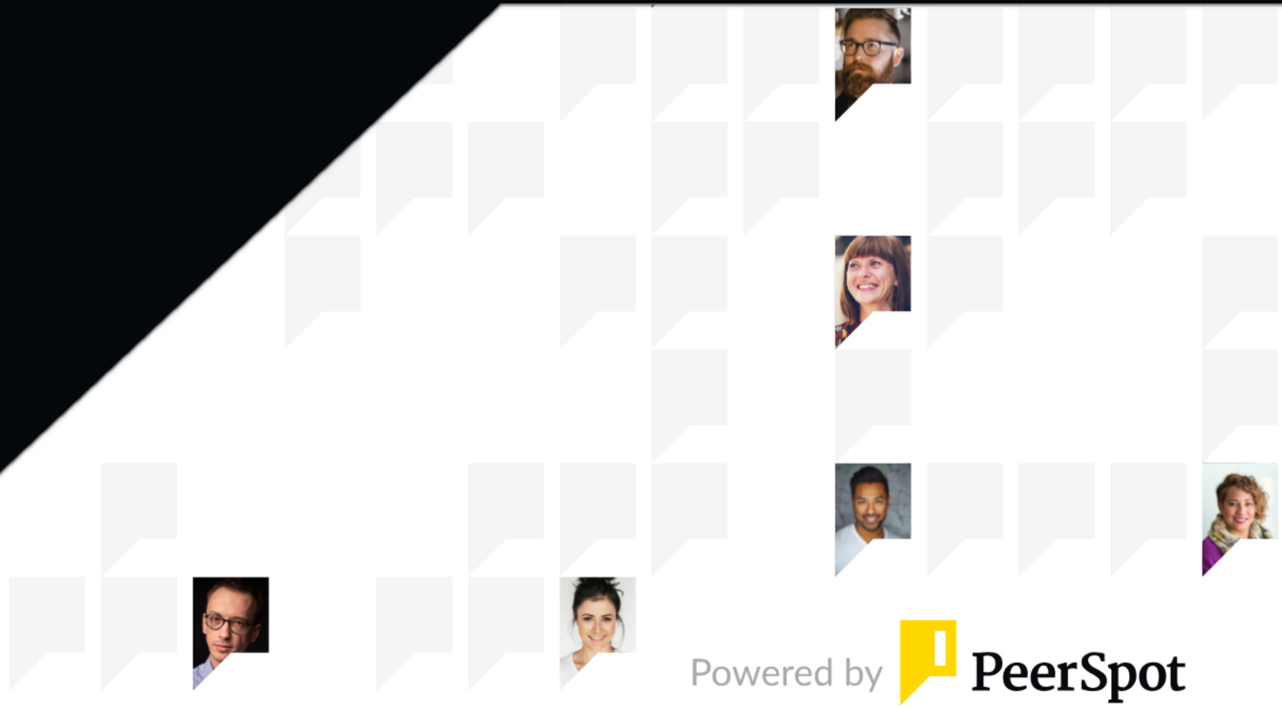
aws marketplace

CrowdStrike Falcon

Reviews, tips, and advice from real users



Powered by PeerSpot

Contents

Product Recap

CrowdStrike Falcon

CrowdStrike Falcon Recap

CrowdStrike Falcon provides AI-powered endpoint detection and protection with minimal system impact. Its real-time monitoring and cloud-native design support efficient threat analysis and integration with other platforms, enhancing security management and workflow.

CrowdStrike Falcon is renowned for its comprehensive cybersecurity features, offering automatic threat analysis and AI-driven protection. Users appreciate its cloud-native flexibility and seamless integration capabilities. Its real-time monitoring, incident response, and vulnerability assessment deliver detailed insights and threat intelligence. Despite its robust features, improvements in integration with other technologies, dashboard functionalities, log management, and support for outdated systems are desired. Enhanced reporting, detailed malware analysis, and reduced false positives can improve user experiences. Organizations leverage Falcon for endpoint protection, threat detection, ransomware defense, and forensic investigations with its effective AI capabilities.

What are the key features of CrowdStrike Falcon?

- Endpoint Detection: Provides comprehensive monitoring and AI-driven analysis to identify threats.
- Automatic Threat Analysis: Uses machine learning to swiftly analyze potential threats.
- AI-Driven Protection: Employs advanced AI for proactive security measures.
- Real-Time Monitoring: Offers immediate detection and alerting of security issues.
- Incident Response: Facilitates efficient response to security incidents and breaches.
- Vulnerability Assessment: Identifies and evaluates security vulnerabilities effectively.
- Seamless Integration: Easily connects with other platforms for unified security management.
- Threat Intelligence: Provides in-depth insights into security threats and activities.

What benefits should users look for in reviews?

- Minimal Performance Impact: Ensures systems run efficiently without significant resource use.
- Cloud-Native Flexibility: Offers scalable and adaptive use without on-premises constraints.
- Detailed Insights: Provides comprehensive data for informed decision-making and threat assessment.
- Robust Protection: Keeps evolving threats at bay with customizable policies and frequent updates.
- Enhanced Workflow: Improves user productivity with an efficient, streamlined dashboard.

In finance and healthcare, CrowdStrike Falcon is implemented to protect against advanced threats and ensure compliance. Its AI-driven capabilities aid in real-time threat detection and vulnerability management, making it an essential tool for companies aiming to secure sensitive data and maintain operational continuity. Manufacturing sectors utilize it for securing production systems against potential cyber threats, ensuring uptime and safety. CrowdStrike Falcon's adaptable architecture benefits these industries by providing reliable protection across varied operating environments.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

✓ “The most beneficial part is the active response capability of the product.”

Waleed Omar

Information Security Specialist at Arab Open University

✓ “CrowdStrike is a great solution.”

Sumanth Kandanuru

Security Analyst at NTT Ltd

✓ “The machine learning behavior for anomaly detection is a valuable feature. It helps identify any suspicious or unusual activities within the system.”

Shubham Sinha.

Senior Principal Information Security Analyst at Veritas Technologies LLC

✓ “EDR is effective in CrowdStrike.”

Bhim Arora

Group Manager at HCLSoftware

✓ “CrowdStrike Falcon serves as a next-gen AV, which basically does AI-based behavioral analysis to detect and act on malware or ransomware.”

Jai Prakash Sharma

Vice President, Technology Operations at InfoEdge India Ltd

✓ “The most beneficial features of CrowdStrike Falcon are that it is easy to install, easy to manage, lightweight, and it can stop breaches.”

BambangTrisilo

IT consultant at Asuransi Ramayana

✓ “I find nothing to miss in terms of stability; there are no glitches, and the solution is stable.”

Bhupesh-Sharma

Large account Manager at Softcell Technologies Limited

What users had to say about valuable features:

“CrowdStrike Falcon has many valuable features. The solution is used for multiple functions, including MDR, XDR, and CNA solution. It depends on which category you're looking for, and you have to customize the customer's equation accordingly.

CrowdStrike Falcon can be deployed both on-premise and in the cloud, and it's an on-call solution that can be deployed anywhere by simply deploying the agent on the end devices..”

Bhupesh-Sharma

Large account Manager at Softcell Technologies Limited

Read full review ↗

“The most beneficial part is the active response capability of the product. Being an EDR solution, it helps us identify attacks in real-time. The product runs in the background 24/7. The most interesting aspect is the behavior analysis functionality, which analyzes the behavior of any suspicious activity.

“It identifies threats efficiently due to its built-in intelligence and AI capabilities, which has been extremely helpful for our organization..”

Waleed Omar

Information Security Specialist at Arab Open University

Read full review ↗

“The features I appreciate the most are numerous; the overall product is very good, actually.

“This is an advanced tool in terms of AI which is implemented and integrated. CrowdStrike Falcon has a ransom detection time of less than 50 seconds. Detection and taking down violations and breaches takes a minimum time of 59 seconds. Intelligence is very good, as AI is integrated with this solution. The integration capabilities in CrowdStrike Falcon are very good..”

Rojal Barreto
Computer Engineer at OIC, Alshirawi

Read full review

“The CrowdStrike Falcon has enhanced our cybersecurity posture in our organization by providing full visibility for each endpoint.

“The real-time analytics aspect of CrowdStrike performs well because we get all logs in real-time, with no delay, allowing us to take action immediately.

“The integration capabilities of CrowdStrike are excellent; we can integrate it with many SIM solutions and SOAR, and we have already integrated with different platforms. While integrating it with other platforms, I do not remember facing any issues, as we have a very good team for custom connectors, and the integration is smooth without any challenges..”

Mahmoud Younes
CyberSecurity Architects at VaporVM

Read full review

“The most beneficial features of CrowdStrike Falcon are that it is easy to install, easy to manage, lightweight, and it can stop breaches.

“The impact of CrowdStrike Falcon lightweight agents on system performance and visibility is good, with only one agent required.

“Speaking about the utilization of Falcon threat graph for threat hunting, it helps my security team to predict and prevent potential breaches.

“Considering that CrowdStrike Falcon is a cloud-native architecture, the elimination of on-premises infrastructure makes cybersecurity maintenance cost and complexity minimal, because we only need to install it and then monitor from the dashboard..”

BambangTrisilo
IT consultant at Asuransi Ramayana

Read full review ↗

“For threat detection, the most effective feature I find in CrowdStrike Falcon is 24/7 managed monitoring, which is basically a next-gen antivirus and next-gen endpoint detection and response. In endpoint detection and response, the best part is 24/7 365 continuous monitoring to the endpoint for identifying any suspicious activity.

“CrowdStrike Falcon serves as a next-gen AV, which basically does AI-based behavioral analysis to detect and act on malware or ransomware.

“The automated response capabilities in CrowdStrike Falcon handle incidents based on the behavior of the activity, performing analysis in case it finds more objectionable content. If there is blocking or breaking any of your site map or something of that sort, it is an untraditional way. If the traffic behaves suspiciously, it triggers an automated response to block it. Additionally, if it detects a file which might have an extension of MIME type of maybe a document whereas it is self-replicating, that sends a suspicious activity alert. In such cases, the detection happens automatically. Because in case it's a zero-day, many times such files automatically get put in a sandbox to extract it and see why it is identified as malware. It offers automated threat detection as well, not only automated response.

“Falcon's integration capabilities with other tools enhance my security posture because it has a very lightweight agent, and having a unified console gives us complete visibility, including endpoints, servers, containers, cloud workloads, everything..”

Jai Prakash Sharma

Vice President, Technology Operations at InfoEdge India Ltd

Read full review

Other Solutions Considered

“We evaluated several other options before choosing CrowdStrike. Our decision was based on the product's effectiveness and ability to meet our security requirements..”

Mahmoud_Yassin
CTSO at Cyb3r

Read full review ↗

“I used McAfee before CrowdStrike Falcon for the same use case. I switched to CrowdStrike Falcon because McAfee did not have machine learning or AI capabilities at that time..”

BambangTrisilo
IT consultant at Asuransi Ramayana

Read full review ↗

“I have used SentinelOne as well. SentinelOne was similar but had major challenges with workflow implementation. Workflow implementation is far easier in CrowdStrike compared to SentinelOne..”

Shubham Sinha.
Senior Principal Information Security Analyst at Veritas Technologies LLC

Read full review ↗

“I used McAfee before CrowdStrike Falcon for the same use case. I switched to CrowdStrike Falcon because McAfee did not have machine learning or AI capabilities at that time..”

BambangTrisilo

IT consultant at Asuransi Ramayana

Read full review

“I do not see a lot of advantages in CrowdStrike Falcon; however, because of one particular problem, we had to give away SentinelOne. Otherwise, all three products are quite comparable..”

Jai Prakash Sharma

Vice President, Technology Operations at InfoEdge India Ltd

Read full review

“Before CrowdStrike, I worked with other solutions for EDR and XDR, specifically Trend Micro and Microsoft Defender's Endpoint, as we are working in MSSP.

“The main differences between CrowdStrike and Trend Micro or Microsoft solutions are that CrowdStrike gives me more visibility, while with Defender, I have to run queries which are not easy to use. Even network telemetry for CrowdStrike is very simple and easy to read, allowing for faster understanding compared to Defender where creating rules requires more tuning. Regarding disadvantages of CrowdStrike in comparison to Defender or Trend Micro, I do not see any..”

Mahmoud Younes
CyberSecurity Architects at VaporVM

Read full review

ROI

Real user quotes about their ROI:

“As for return on investment after implementing CrowdStrike Falcon, I would say if it is protecting my environment, that itself meets my expectations so far..”

Jai Prakash Sharma
Vice President, Technology Operations at InfoEdge India Ltd

Read full review

“When we track the annual priority cases, especially the security incidents, we have made many improvements. That is ROI in terms of tracking security incidents..”

Sanjay Dahiya
Global IT Infrastructure Manager at TMF Group

Read full review

“We have not calculated the ROI extensively, as we typically only calculate it when there is dissatisfaction. On a scale of one to ten, the ROI would be five, which translates to approximately 60%..”

Waleed Omar
Information Security Specialist at Arab Open University

Read full review

“On the terms of investigating, I find it's quite easy to investigate an event and have a broader look at the event using CrowdStrike. I would rate the time saved around eight, nine, or even ten out of ten. Compared to Defender, it makes it faster to investigate..”

Verified user

IT Specialist at a consultancy with 1-10 employees

Read full review

“CrowdStrike Falcon saves time and offers good value for money, especially for enterprise companies, because it can stop breaches.

“I am not sure about the exact percentage of money it saves, as I have to calculate the risks, but we are satisfied because CrowdStrike Falcon has stopped breaches and prevented hackers..”

BambangTrisilo

IT consultant at Asuransi Ramayana

Read full review

“The benefit I've seen is their backend, which powers the EDR, XDR, and NGAV. It's really good because it can detect anything due to the wide range of customers they have.

For example, one customer has a vulnerability because of a zero-day attack. All the other customers will benefit because it propagates to the cloud and analyzes if other customers are on the same version of the drivers or any other Windows patch. If they are, it will tell us that there's an issue and provide remediation steps. Many of our customers find this very helpful. It's called the CrowdStrike community..”

Abhishek A

Trainee Engineer at COMPASS IT Solutions & Services Pvt.Ltd.

Read full review

Use Case

“The typical use case for CrowdStrike Falcon depends on what kind of service the customer is looking for. Most customers look for antivirus, endpoint detection and response, or possibly managed detection and response, which leads them to reach out to us.

When we speak to the customer, they usually tell us that they're looking for antivirus or endpoint detection and response, and we then introduce CrowdStrike Falcon..”

Bhupesh-Sharma
Large account Manager at Softcell Technologies Limited

Read full review

“We are using it for endpoint protection, as well as for cloud security coverage. It includes monitoring all our critical servers and endpoint devices. We also design workflows for anomaly behavior detection using machine learning techniques for anything malicious or abnormal. We monitor everything suspicious. We either design the workflows or use CrowdStrike to monitor any new detections and anomaly behaviors, as well as do vulnerability management..”

Shubham Sinha.
Senior Principal Information Security Analyst at Veritas Technologies LLC

Read full review

“We are protecting our endpoints, workstations, servers, and cloud workloads. This includes effective use of antivirus and detection and response capabilities.

“I am working at Arab Open University, and we are using CrowdStrike Falcon as our security product..”

Waleed Omar
Information Security Specialist at Arab Open University

Read full review

“For our use cases, we are using it to collect IOCs, and we also are using EDR, with injection integrated with our SIM solution to create some use cases.

“What I find beneficial about CrowdStrike Falcon is that it performs effectively. We are focusing only on EDR and creating use cases regarding user processes or endpoints, particularly user behavior analytics..”

Mahmoud Younes
CyberSecurity Architects at VaporVM

Read full review

"In my cybersecurity strategy, I use CrowdStrike Falcon mainly as an EDR solution for us. Currently, we are using it as an EDR. We are also in discussion along with the CrowdStrike team where we can have a managed SOC integrated.

"In the online industry, we are using CrowdStrike Falcon, specifically in online classified, which you could call e-commerce.."

Jai Prakash Sharma
Vice President, Technology Operations at InfoEdge India Ltd

Read full review

"I am currently using CrowdStrike Falcon as an EDR, which is integrated with SIEM. We also work in a real-time environment with the product. As a Falconist, I perform investigation actions on it. There are three different kinds of alerts I deal with: one based purely on IOCs, another process-oriented IOA, and those based on machine learning alerts. This is what I work on, and it is actually a good tool. It has multiple features, including real-time connection to the RTR environment, allowing direct remote host connection through CrowdStrike. I have multiple options like host search and event search, enabling me to do everything I need. It's a comprehensive package. It's a challenging tool to explore, but once accustomed to it, it is quite excellent.."

Sumanth Kandanuru
Security Analyst at NTT Ltd

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.

"I was not involved in the implementation part of CrowdStrike in my environment because I arrived after it was already installed, so I did not start from scratch.."

Mahmoud Younes

CyberSecurity Architects at VaporVM

Read full review

"CrowdStrike Falcon can be deployed both on-premise and in the cloud, and it's an on-call solution that can be deployed anywhere by simply deploying the agent on the end devices.."

Bhupesh-Sharma

Large account Manager at Softcell Technologies Limited

Read full review

“The current setup is easy, but it could be more natural and make drill-down searches simpler. With advancements in AI, integration could streamline responses further, but there is still room for making the process easier..”

Sumanth Kandanuru

Security Analyst at NTT Ltd

Read full review

“The setup is straightforward, and most of our integration is within the package. However, for the integration part, we need to purchase additional modules from CrowdStrike Falcon. If this functionality was included as a free standalone feature within the built-in solution, it would be more market competitive. Competitors such as SentinelOne and Microsoft Defender provide this functionality out of the box without additional charges..”

Waleed Omar

Information Security Specialist at Arab Open University

Read full review

“CrowdStrike Falcon is fairly easy to set up, according to my experience and our team's experience. Since we have a heterogeneous environment, for Windows it is very straightforward and easy, but for Linux it is a bit complex since you need to automate it. If you have a bulk force, then you have to use some CMF or something similar. Overall, it is still fairly easy.

“For deployment, it takes approximately a couple of minutes..”

Jai Prakash Sharma

Vice President, Technology Operations at InfoEdge India Ltd

Read full review ↗

“We have it in the on-premises environment and cloud environments. For endpoint hosts, it is very easy, but in the cloud environment, there are challenges, especially if we have AWS technologies with Lambda functions, which are serverless.

My implementation strategy was simple. I segregated servers based on criticality, then network, and finally OS level. Anything critical was based on my CMDB asset configuration. Following criticality was the network, determining internal versus public-facing. The last segmentation was on OS configuration. These three categorizations were primarily used in deploying agents across our environment.

In terms of maintenance, there are patches or version upgrades. .”

Shubham Sinha.

Senior Principal Information Security Analyst at Veritas Technologies LLC

Read full review ↗

Customer Service and Support

“The customer service is good and efficient in terms of responding. They could improve by initiating calls for high-priority cases instead of just opening tickets. When we open a support ticket, they should call to discuss what happened and listen to our concerns..”

Waleed Omar
Information Security Specialist at Arab Open University

Read full review

“We have a Technical Account Manager (TAM). We can directly call them and raise a ticket. Initially, it was a six or even a five because we had to send an email, and it would take three to four days for them to reply. Now, with the TAM, we can get issues resolved faster..”

Abhishek A
Trainee Engineer at COMPASS IT Solutions & Services Pvt.Ltd.

Read full review

“I have contacted CrowdStrike for issues, and the response was poor. That particular experience was pretty bad, with people not knowing what was happening, how to mitigate, or what to do. We were in a bad situation, but after a couple of hours, their communication started flowing fine, and things gradually started improving. For that particular instance, I would rate it less than four..”

Jai Prakash Sharma

Vice President, Technology Operations at InfoEdge India Ltd

Read full review

“Technical support depends on a system integrator.

CrowdStrike technical support regarding Identity Protection has a team, but if there's no issue with the agent, you can work it out yourself.

The support is good..”

Bhupesh-Sharma

Large account Manager at Softcell Technologies Limited

Read full review

“Technical support from CrowdStrike Falcon is good because usually in Indonesia we have a partner, and if the partner cannot address the issue, we discuss with CrowdStrike directly.

“I would rate technical support a nine out of ten..”

BambangTrisilo
IT consultant at Asuransi Ramayana

Read full review

“Regarding maintenance, the service is excellent; if we face any issues, we open a ticket with the CrowdStrike support team.

“I would evaluate CrowdStrike tech support as excellent because they have a very fast response.

“On a scale of one to ten, I would rate the technical support as a 10 because they resolve many issues for us..”

Mahmoud Younes
CyberSecurity Architects at VaporVM

Read full review

Other Advice

“My rating for CrowdStrike Falcon would be eight points because there are many antivirus competitors. For those who want to use CrowdStrike Falcon, they should be mindful of the higher price compared to others..”

BambangTrisilo
IT consultant at Asuransi Ramayana

Read full review

“CrowdStrike is a great solution. It's a hands-on tool. I have not seen other EDRs like it. Compared to Carbon Black, which is much more difficult with a different UI, CrowdStrike allows direct, detailed investigation with a PID generated for each process. It offers unique abilities not seen in other EDRs. Overall product rating: nine out of ten..”

Sumanth Kandanuru
Security Analyst at NTT Ltd

Read full review

"I would rate CrowdStrike Falcon an eight out of ten. They have some challenges with the cloud environment, which is a major drawback, especially with the serverless aspect. Their GUI also causes issues with regular changes.

If anyone has worked with CrowdStrike, they would promote it. However, cloud security presents challenges. Moving from physical to cloud environments is difficult. I have raised 7-8 tickets to resolve cloud issues, especially with AWS.."

Shubham Sinha.
Senior Principal Information Security Analyst at Veritas Technologies LLC

Read full review

"We are part two of CrowdStrike. The time it takes to deploy CrowdStrike Falcon depends on the customer setup.

My clients vary in size, as we can reach all types of businesses, whether small, medium, or enterprise.

Based on my experience, I would recommend CrowdStrike Falcon solutions to other people. I rate the solution an eight out of ten.."

Bhupesh-Sharma
Large account Manager at Softcell Technologies Limited

Read full review

“For those who would like to use CrowdStrike Falcon, I recommend negotiating hard on commercial terms because it is not an easy or affordable solution. From a commercial standpoint, you should negotiate hard, but technically, it is not very difficult.

“CrowdStrike Falcon is a user-friendly tool.

“On a scale of one to ten, I rate CrowdStrike Falcon an eight..”

Jai Prakash Sharma
Vice President, Technology Operations at InfoEdge India Ltd

Read full review

“Based on my experience, I would recommend CrowdStrike to others because it is user-friendly and easy to manage, unlike other solutions that require experienced personnel; CrowdStrike's documentation is also very clear.

“I would recommend it to other users because it is a perfect product.

“It is an easy solution that anyone can manage, providing many benefits for endpoint visibility and allowing for the creation of many custom use cases without the need for much fine-tuning to get true positive alerts.

“On a scale of one to ten, I would rate CrowdStrike Falcon as a product and solution as an eight..”

Mahmoud Younes
CyberSecurity Architects at VaporVM

Read full review

Top Industries

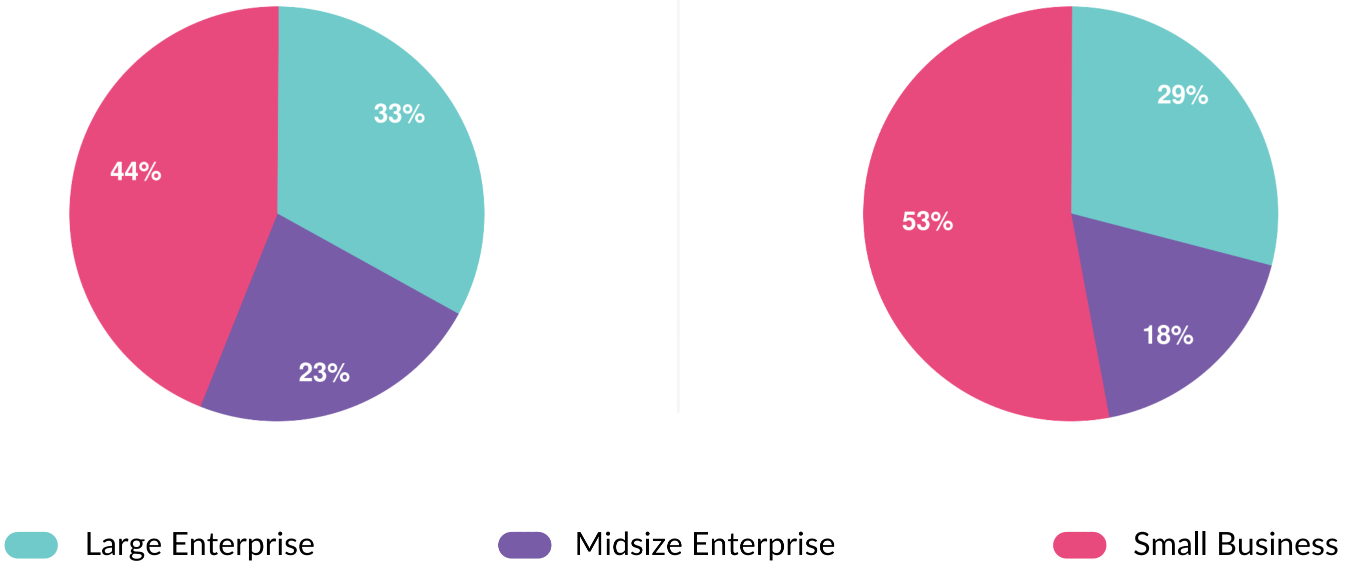
by visitors reading reviews

Computer Software Company	15%
Financial Services Firm	10%
Manufacturing Company	9%
Government	6%

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