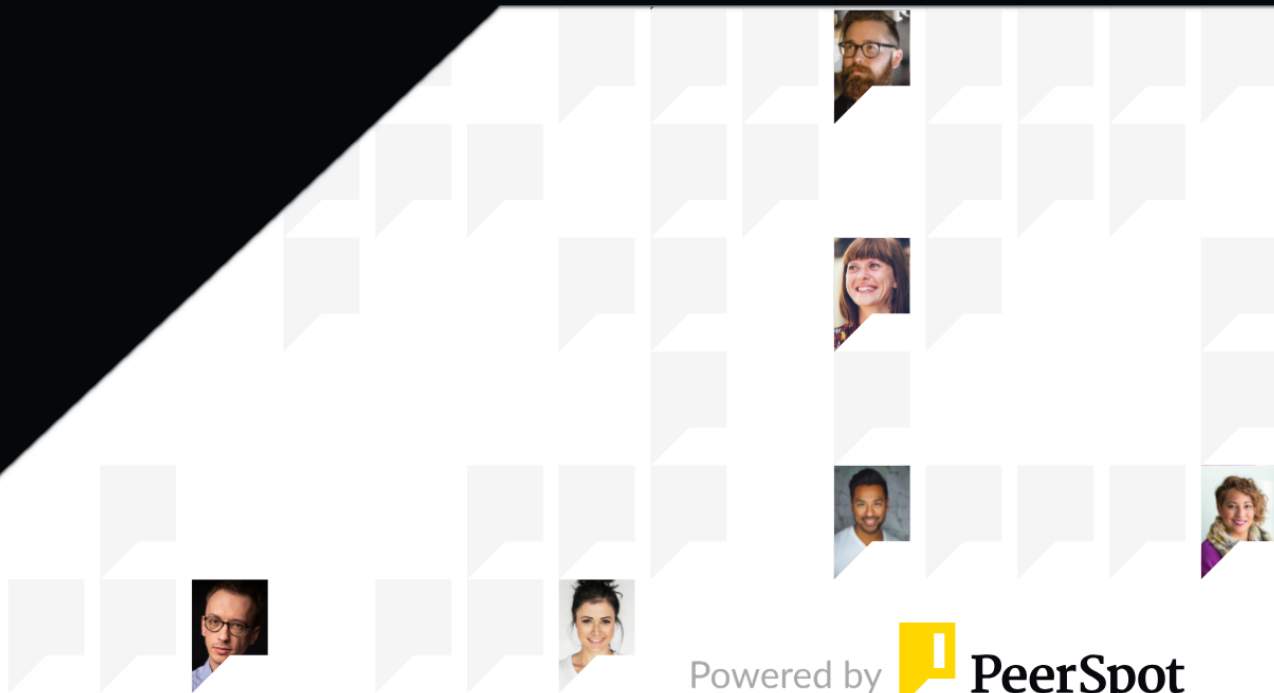


aws marketplace

Sublime Security

Reviews, tips, and advice from real users



Powered by  **PeerSpot**

Contents

Product Recap..... 3 - 5

Valuable Features..... 6 - 13

Other Solutions Considered..... 14

ROI..... 15

Use Case..... 16 - 20

Setup..... 21

Customer Service and Support..... 22

Other Advice..... 23 - 26

Trends..... 27 - 28

About PeerSpot..... 29 - 30

Product Recap



Sublime Security

Sublime Security Recap

Sublime's agentic platform stops more email attacks with less work. Our AI agents work like a digital SOC team in your environment, triaging and blocking advanced threats while adapting protections at adversary speed. It provides full transparency and automation by default, with control on demand for advanced teams, eliminating vendor bottlenecks or one-size-fits-all limits.

Core Outcomes (The What):

- Stop More Attacks with Fewer False Positives - block sophisticated threats (BEC, novel phishing, QR-based phishing) and reduce the false positives that waste time and disrupt workflows. Our tailored protections deliver a demonstrably higher catch rate, validated by the world's most demanding security teams.
- Automate the Abuse Mailbox - Our Autonomous Security Analyst (ASA) automates triage, investigation, and remediation of user-reported email, cutting MTTR from hours to seconds and freeing your SOC team to focus on the threats that matter most.
- Adapt Defenses Automatically. - When a missed attack is identified, we can create new coverage in hours. Our Autonomous Detection Engineer (ADÉ) generates, backtests, and deploys org-specific coverage, eliminating vendor ticket limbo.

Differentiators (The How):

- A Team of Agents using AI, Not Just a Black Box - Sublime deploys a team of specialized agents - like an analyst and a detection engineer - that use AI to protect, triage, and adapt your defenses. Unlike an opaque, monolithic AI, our agentic approach provides full transparency into every action, with visible decision history, message lineage, and backtests.
- Org-Specific Protection, Not One-Size-Fits-All - Our Distributed Detection Model (DDM) is the foundation of our platform. It runs per-environment coverage that adapts to the unique attacks you face, allowing us to safely deploy protections that would be noisy in global models - something centralized systems simply can't support. This means higher day-one efficacy and fewer false positives.
- Autonomous by Default, Control on Demand - By stopping more attacks and reducing false positives, Sublime delivers a superior autonomous experience that requires less work. For advanced teams, the platform is fully extensible, allowing you to author your own detections and hunt for threats with a level of precision that one-size-fits-all solutions can't.

Innovative organizations including Spotify, Snowflake, Brex, Elastic, Compass, Anduril, SentinelOne, and others rely on Sublime to secure the business and keep teams focused on strategic defense.

Valuable Features

Excerpts from real customer reviews on PeerSpot:



“Overall, the auditability and the ability to evaluate the information in Sublime through various mechanisms made me very comfortable with setting these capabilities to auto-remediation.”



Verified user

Manager Security Operations Center at a educational organization with 10,001+ employees



“Sublime Security has positively impacted our organization by allowing us to do much less manual phishing detection and email detection, and now we can automate a lot of that, freeing up a lot of our security team to do other work.”



Connor

Technical Lead at a consultancy with 11-50 employees



“Sublime Security has positively impacted my organization by helping our team reduce manual email triage and respond to phishing and BEC threats faster.”



Vsadalaga Sadalga

Soc Analyst at a manufacturing company with 10,001+ employees

- ✓ “Sublime Security has improved our email threat detection and response by helping us identify phishing and Business Email Compromise campaigns faster, investigate related emails, and automate remediation, which has reduced our manual effort and improved our response time.”



Verified user

Soc Analyst at a manufacturing company with 10,001+ employees

- ✓ “This is why it provides absolute value; it adds a smarter layer that catches anything missed by Microsoft 365 or Google Workspace protection, as attackers can breach those systems easily using flexible detection logic that security teams can quickly customize.”



Verified user

Partner Account Manager at a wholesaler/distributor with 51-200 employees

- ✓ “Since I have been using Sublime Security personally, I have noticed specific improvements like fewer spam emails and improved detection, which saves me time.”



Verified user

Associate Software Engineer at a computer software company with 201-500 employees



“I like its ability to detect and block.”



LARK IT

Head of IT at a manufacturing company with 51-200 employees

What users had to say about valuable features:

“What I appreciate most about Sublime Security is the amount of detail that's provided. I've used Microsoft Defender and, in the past, Proofpoint for similar purposes. Both offer valuable insights, but what stands out about Sublime Security is how accessible the detailed analyses are for the messages that have been evaluated. The tools clearly explain why a specific verdict was assigned to a message. This level of detail is essential for analysts and anyone conducting evaluations, as it helps them understand the specific circumstances of their environment. What may be clearly malicious in one organization could be viewed as legitimate or benign in another. The information provided about flagged emails and the subsequent evaluations offers a comprehensive breakdown of how a particular conclusion was reached, which has been incredibly beneficial..”

Verified user

[Read full review](#)

Manager Security Operations Center at a educational organization with 10,001+ employees

“The standout features of Sublime Security revolve around its ability to catch advanced threats that bypass native defenses. Specifically, it excels at blocking malware attachments and stopping Business Email Compromise (BEC), such as CEO fraud and invoice scams.

A major advantage is its fast time-to-value because it isn't a rip-and-replace solution. Instead, it acts as a 'smarter layer' that enhances existing protections like Microsoft 365 or Google Workspace. While native security catches the obvious junk, Sublime uses flexible, customizable detection logic to catch the highly sophisticated attacks that easily slip through standard filters.

Finally, the platform gives you deep visibility and fast search capabilities across all email activity. Without a tool like this, investigations take far too long, and teams lack visibility into what actually breached the inbox. Sublime solves this by offering rapid detection, automated response actions, and the ability to quickly remove malicious emails in bulk..”

Verified user

[Read full review](#) 

Partner Account Manager at a wholesaler/distributor with 51-200 employees

In my opinion, the best features of Sublime Security are advanced phishing and BEC detection, campaign grouping, threat hunting, and automated remediation. I especially find campaign grouping and remediation useful because they allow me to investigate related emails together and quickly quarantine or remove malicious messages across affected mailboxes, and Sublime Security provides detailed detection reasoning that aids during my investigations.

Campaign grouping helps us identify similar phishing patterns across multiple users and investigate them as one campaign instead of handling each email separately, which makes it easier to spot common IOCs, understand the attack pattern, and quickly remediate all related messages. This saves our time and improves consistency.

“Sublime Security has improved our email threat detection and response by helping us identify phishing and Business Email Compromise campaigns faster, investigate related emails, and automate remediation, which has reduced our manual effort and improved our response time. This enables us to better protect against email-based threats. .”

Verified user

[Read full review](#) 

Soc Analyst at a manufacturing company with 10,001+ employees

“The best features Sublime Security offers include detection as code, which gives a very powerful feature for users to write rules, custom objects, and the language provides some syntax that is definitely a good feature. The second one is why it detects spam emails or justifies why this is considered spam, which is the second most valuable feature.

“I use the detection as code feature in my day-to-day life, which usually identifies junk emails and spam emails by default with the conditions and the vast dataset it has. Even if some emails may not get into that machine learning dataset, I can describe if it is from an external source and has rewards; I can remove it since it is considered spam. This feature changes the usual segregation and categorization, helping users not fall for known types of emails that the system may not detect. The explanation of justification, instead of just flagging something as spam, gives the user understanding such as, this is not a Google email; we really cannot click on it. It enhances user security, and even if another user sees this type of content based on gesture events for another email, they think not to use the image correctly.

“Sublime Security has positively impacted my organization..”

Verified user

[Read full review](#) 

Associate Software Engineer at a computer software company with 201-500 employees

“I'd say the best features Sublime Security offers are the threat detection and investigation capabilities, which are probably the most valuable part for us. I particularly appreciate the visibility into the email activity and the ability to investigate suspicious messages and understand why something was flagged. I'd say the protection against more sophisticated phishing and business email compromise attacks is also important. Those are difficult to deal with because they don't always contain obvious malware.

“The investigation capabilities of Sublime Security stand out because they surface themselves in a very nice, obvious way. So when we are investigating, they're just easy to spot and easy to identify. The UI is very clear for us, and overall it's just what we would expect.

“Regarding Sublime Security's AI capabilities, I think it's honestly pretty good. I haven't had any issues with either the governance side or the security side.

“I think Sublime Security has been very accurate. For us, it's certainly stopped a lot of the manual investigation that we often do for phishing emails or malicious emails. Occasionally, it does give us false positives, but that's just a five-minute review of something, so it still cuts a lot of time down..”

Connor

Technical Lead at a consultancy with 11-50 employees

[Read full review](#) 

“For me, the best features Sublime Security offers are phishing and BEC detection, detailed email analysis, threat hunting, and automated triage remediation. I appreciate that the detections are transparent, allowing me to understand why an email was flagged instead of just receiving a black box verdict. Sublime Security's AI Analyst is particularly useful for automatically investigating user-reported emails and reducing manual triage work.

“Sublime Security's AI Analyst has helped me reduce the amount of manual email triage I need to do because when users report suspicious emails, it analyzes the message, links, attachments, and sender context and provides a verdict with reasoning. This gives me a quick starting point for investigation instead of reviewing everything manually, which saves time especially when there are a large number of user-reported emails. This allows me to focus my attention on cases that actually need deeper investigation.

“I particularly appreciate the combination of detections, threat hunting, and remediation in one platform. The campaign grouping is useful because I can investigate related emails together instead of treating every message as a separate alert. The transparency of the detections is another strong point as it helps me understand why a message was flagged.

“Sublime Security has positively impacted my organization by helping our team reduce manual email triage and respond to phishing and BEC threats faster. The automated analysis and remediation allow analysts to spend less time reviewing routine user-reported emails and more time on higher-risk investigations. It also gives us better visibility into why an email was flagged, making investigations and escalations easier.

“The biggest measurable impact has been reducing the time spent on email triage, handling user-reported phishing emails faster, and reducing the amount of manual investigation required. Although I don't have a specific organization-wide percentage to share, the improvement is noticeable in analyst workload and response time..”

Vsadalaga Sadalga

Soc Analyst at a manufacturing company with 10,001+ employees

[Read full review](#) 

Other Solutions Considered

“We didn't actually evaluate other options. We started with Sublime Security and found it met all of the objectives we needed, so we were happy to go ahead with it..”

Connor

Technical Lead at a consultancy with 11-50 employees

[Read full review](#) 

“When I compare it to Microsoft Defender in terms of security effectiveness, I would prefer Sublime Security because it is a separate solution from the main stack, which makes it more proactive in identifying and stopping malicious emails..”

LARK IT

Head of IT at a manufacturing company with 51-200 employees

[Read full review](#) 

ROI

Real user quotes about their ROI:

I have seen a reduction in time saved, and I don't know about the direct cost savings. I estimate that we have improved our efficiency, especially for phishing campaigns where we can handle multiple similar emails together, which has reduced repetitive analyst work and improved our response time. Although I don't have specific metrics to mention, I can confirm it has reduced our time to respond and alert.

Verified user

Soc Analyst at a manufacturing company with 10,001+ employees

[Read full review](#) 

“Sublime Security has proven to be a significant advantage for us. We transitioned from relying on a third-party service provided by Cofense for handling user-reported phishing emails to managing everything in-house. This means that our previous relationship with Cofense has ended, and we have fully replaced their services with Sublime, which automates many remediation actions.

Importantly, we didn't need to hire any additional staff; we were able to absorb this responsibility using our existing team. As we activated more functionalities of the tool, our team learned to manage the process effectively. Now, we handle everything internally, utilizing both the tool and our team's processes..”

Verified user

Manager Security Operations Center at a educational organization with 10,001+ employees

[Read full review](#) 

Use Case

“The basic functionality provided by Microsoft Defender and its email protections was insufficient for our needs. While it effectively handled common spam and phishing attempts, we required a solution that could address more sophisticated attacks. After researching the market, we discovered Sublime Security. Our organization expressed considerable interest in tools that utilize LLM and AI agent technologies. After conducting a thorough review, we selected Sublime Security, and we have been using it in our environment ever since..”

Verified user[Read full review](#) 

Manager Security Operations Center at a educational organization with 10,001+ employees

“Our main use case is two-fold. Primarily, as a channel partner, our core focus is channel enablement. We actively pitch, demonstrate, and distribute Sublime Security to our partner network, who then deploy it for end-user organizations. Secondarily, we 'drink our own champagne' by running it internally to protect our own business communications.

When we position it to our partners, we frame it as an advanced email security platform. It goes far beyond traditional junk filtering by actively hunting the sophisticated threats that bypass native defenses—specifically Business Email Compromise (BEC), CEO fraud, invoice scams, fake login pages, and malware attachments..”

Verified user[Read full review](#) 

Partner Account Manager at a wholesaler/distributor with 51-200 employees

“My main use case for Sublime Security is to test how this product works, so I am using this for that purpose.

“For a quick specific example of what I tested with Sublime Security, it detects the emails of the person on this side to check that feature, and there is a feature in Sublime Security that is detection as code, which is an excellent feature that I have noticed in this product. I am talking about eleven hundred, and that detection feature is something where I can explicitly customize mentions of power spam or non-structured email. With our custom permissions, we have it, and getting that notice by word blocking is something very important. It is a great feature that I have been using.

“Regarding my main use case for testing Sublime Security, it is very good, and I fully specify that detection; it is something very extensive with maximum features..”

Verified user

[Read full review](#) 

Associate Software Engineer at a computer software company with 201-500 employees

“Our primary use case for Sublime Security is email security, so we use Sublime Security to protect Microsoft 365 email against phishing, business email compromise, any malicious links and attachments, and other email-based threats. We're particularly interested in threats that can get through the traditional email security because they don't necessarily look like conventional spam or malware.

“Sublime Security has given our security team better visibility into what's happening in our email environment, and it has actually helped us identify suspicious messages more quickly. For example, one of the benefits is that we're able to investigate email threats without relying entirely on users reporting those suspicious messages. The security team at Cloudhouse can actually see patterns and indicators across the environment and respond accordingly. It has actually reduced the manual investigation work as well..”

Connor

Technical Lead at a consultancy with 11-50 employees

[Read full review](#) 

My main use case for Sublime Security is to detect email threats and respond to them, primarily for investigating phishing and business BEC attempts, analyzing suspicious URLs and attachments, and taking remediation actions on the malicious emails.

I usually start by reviewing the sender, then proceed with header analysis, URL and attachment review, and analyzing the message content. After that, I check the threat indicators and detection results to understand the risk, and if it is confirmed, I use Sublime Security's remediation capabilities to remove or quarantine the email and document the incident.

“I also use Sublime Security to investigate similar email campaigns and identify patterns across users. Its detection and remediation capabilities help me respond consistently, reducing manual work and improving the overall security posture. .”

Verified user

[Read full review](#) 

Soc Analyst at a manufacturing company with 10,001+ employees

“My main use case for Sublime Security is email security and phishing detection, where I use it to investigate suspicious emails, identify phishing and BEC attempts, analyze malicious links and attachments, and support the triage and remediation process.

“One example of how I used Sublime Security to handle a real situation is when it flagged a phishing email that appeared to come from a legitimate vendor based on the sender and email content. I used it to investigate the links and other indicators, confirmed it was a phishing attempt, and removed the message from affected mailboxes, which helped prevent users from interacting with it.

“I mainly use Sublime Security as part of my day-to-day email alert triage, which helps me quickly identify suspicious emails, investigate phishing and BEC attempts, and gather useful context before deciding whether to close or escalate an alert. I also find the automation and remediation capabilities helpful for reducing manual work..”

Vsadalaga Sadalga

Soc Analyst at a manufacturing company with 10,001+ 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.

“It's very simple. You just need to gain API-level access to a Microsoft 365 tenant or a Google Workspace account. As long as someone can provide an API key with the necessary permissions, that's all it takes. The entire process of setting it up is straightforward and easy to implement.

It could take about a week to get the right approvals because of the large organization, but the actual technical implementation takes 30 minutes.

Maintenance is taken care of by Sublime. They do auto updates and addition of new rules and all of that. It's completely hosted by them. It's a full SaaS model..”

Verified user

[Read full review](#) 

Manager Security Operations Center at a educational organization with 10,001+ employees

Customer Service and Support

“Support for Sublime Security has generally been good. People we've dealt with have been knowledgeable about email security and they're able to understand the context of an incident rather than just treating it as a generic support ticket. There have been occasions where we would have liked a faster response, but the overall experience has been positive.

“I would probably rate the customer support as a nine out of ten..”

Connor

Technical Lead at a consultancy with 11-50 employees

[Read full review](#) 

“We have a Teams channel that we use regularly with them. They provide updates on new capabilities being enabled, as well as information that allows us to open cases if we have questions. If there's an issue in the platform that they want us to investigate further, this communication channel allows for free-flowing dialogue.

I haven't been disappointed so far; their response is very fast. If there's something more complex, they can connect you with the appropriate engineering resources for a more in-depth conversation. We have our own internal AI review panel, and we were able to get in touch with the person who constructed the LLM and its agentic aspects relatively quickly to address our questions. They offer a wide range of expertise to their customer base on relatively short notice. Overall, they have been highly responsive and very helpful. .”

Verified user

Manager Security Operations Center at a educational organization with 10,001+ employees

[Read full review](#) 

Other Advice

My advice to others looking into using Sublime Security is to start with a focused use case such as phishing or user-reported email triage, integrate it with your existing Microsoft 365 or [Google Workspace](#) environment, tune the detection based on your needs, and then gradually enable automated remediation. I would rate this product nine out of ten.

Verified user

Soc Analyst at a manufacturing company with 10,001+ employees

[Read full review](#) 

“I would recommend Sublime Security to teams that want to strengthen their existing email security and reduce manual phishing triage. I suggest they start with a focused evaluation using real user-reported emails and measure detection quality, false positives, and analyst time saved. I have covered all the relevant points regarding Sublime Security. I give this product a rating of 9..”

Vsadalaga Sadalga

Soc Analyst at a manufacturing company with 10,001+ employees

[Read full review](#) 

“I haven't experienced any significant reliability issues or any issues at all. Sublime Security is normally pretty accurate in its detection. I appreciate the AI capabilities and the UI. I'm sure there is something that can be improved to make my life even better that I don't yet realize.

“I recommend that you define your email security requirements before starting the evaluation. I would rate Sublime Security a nine out of ten..”

Connor

Technical Lead at a consultancy with 11-50 employees

[Read full review](#) 

“On a scale of one to ten, I rate [Sublime Security](#) a nine out of ten because I believe there are a couple of negatives regarding scalability for catering to enterprise and small to medium enterprises. Additionally, the product requires a learning phase, and it is not readily usable right away.

“ [Sublime Security](#) merits this rating because of a couple of changes that need to be addressed. If it catered to both small and enterprise businesses on a pricing scale, it would receive a ten, but it is not far away..”

Verified user

Partner Account Manager at a wholesaler/distributor with 51-200 employees

[Read full review](#) 

“We have not yet fully enabled ADÉ, but I am working on getting it activated because we have confidence in the rest of the toolset and its available functions. Currently, it is undergoing evaluation and remains in public beta. For any components that we activate, particularly those based on AI, we have an internal review board. This board focuses on determining whether a large language model

(LLM) or AI component will be used to facilitate model learning in other environments or if it will be restricted solely to our tenant. We want to ensure that our internal organizational messages are not used to train external models. This review process will be conducted on a function-by-function basis, even for tools we've previously assessed. Although we haven't completed this review for the component yet, it is on our agenda. I would like to have it turned on before the end of the calendar year. We are moving forward with this, but it must pass our internal review first. If the review results are positive, we will aim to enable it before the end of December.

I would rate Sublime Security a nine out of ten..”

Verified user

Manager Security Operations Center at a educational organization with 10,001+ employees

[Read full review](#) 

“Phishing versus phishing detection is also something I find good, and I have mentioned these things already.

“Since I have been using Sublime Security personally, I have noticed specific improvements like fewer spam emails and improved detection, which saves me time. It helps me segregate emails instead of reviewing all things manually, as it detects spam emails. I do not have to go through every email, which makes me very efficient for other tasks. It also shows if some emails are current, and if I am about to register or receive registration links, it tells me why those emails are separated. I understand better instead of reading all the emails, and it summarizes the words or thumbnails of the emails. If an email is considered good, I continue, making my time more efficient.

“Regarding the AI capabilities of Sublime Security, I think for detection, using ML to analyze content is already a feature present in Sublime Security, which also identifies phishing attempts.

“I think Sublime Security shows false positives. I give this review a rating of nine..”

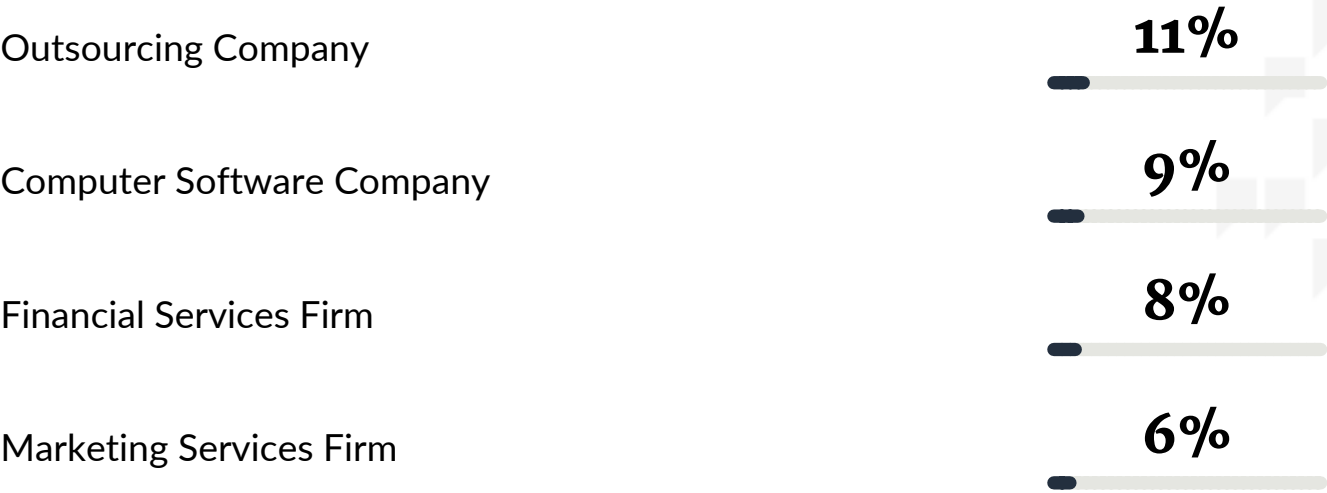
Verified user

Associate Software Engineer at a computer software company with 201-500 employees

[Read full review](#) 

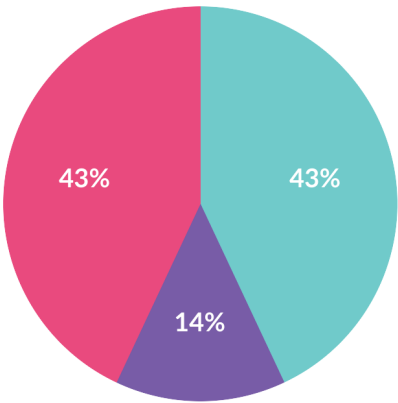
Top Industries

by visitors reading reviews

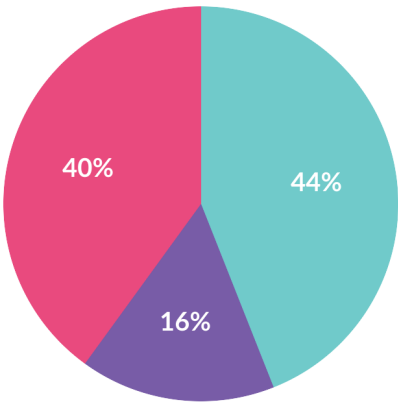


Company Size

by reviewers



by visitors reading reviews



Large Enterprise Midsize Enterprise Small Business

About this buyer's guide

Thanks for downloading this PeerSpot report.

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

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

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

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

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

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

[Get your personalized report here](#)

About PeerSpot

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

PeerSpot helps tech professionals by providing:

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

Use PeerSpot to:

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

Join PeerSpot to connect with peers to help you:

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

Visit PeerSpot: www.peerspot.com

PeerSpot

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

reports@peerspot.com

+1 646.328.1944