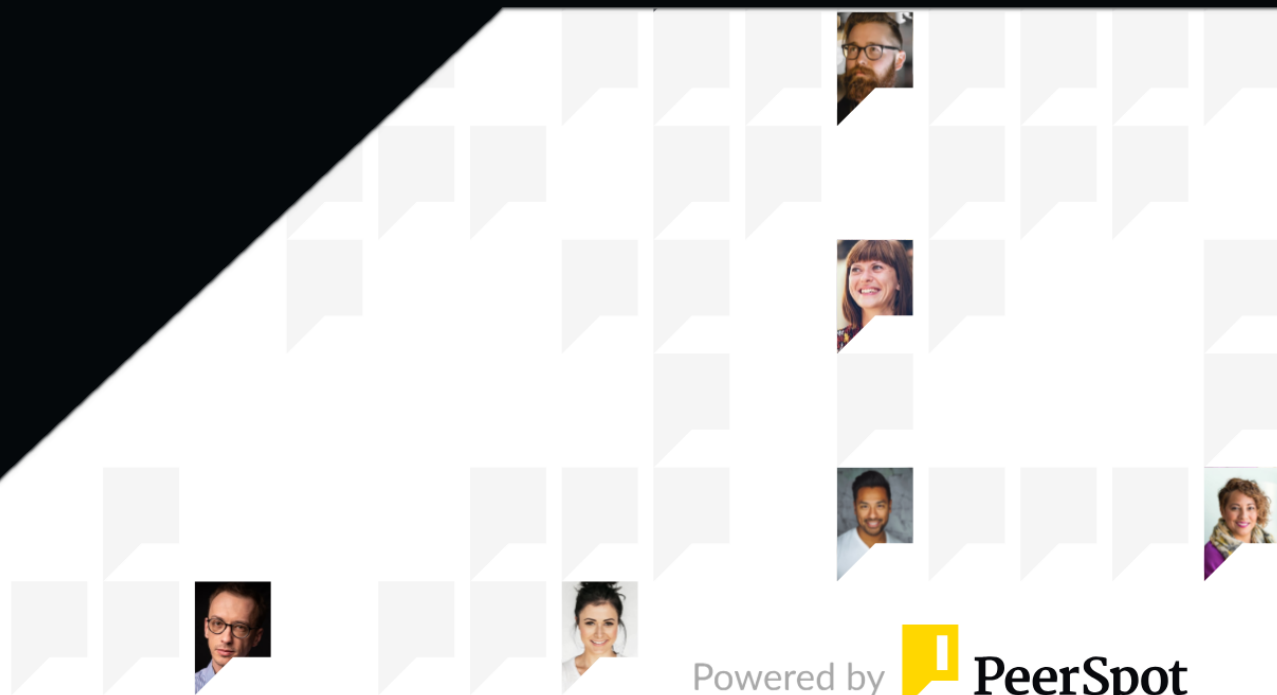




**Codebashing**

# **Reviews, tips, and advice from real users**



Powered by  **PeerSpot**

# Contents

Product Recap..... 3 - 4

Valuable Features..... 5 - 10

Other Solutions Considered..... 11 - 13

ROI..... 14 - 15

Use Case..... 16 - 19

Setup..... 20 - 22

Customer Service and Support..... 23 - 25

Other Advice..... 26 - 28

Trends..... 29 - 30

About PeerSpot..... 31 - 32

# Product Recap



Codebashing

# Codebashing Recap

Codebashing provides comprehensive security training, focusing on real-time remediation, vulnerability discovery, and improved development practices through adaptive learning and gamification.

Codebashing offers a dynamic approach to developer training, emphasizing security from the onset of application design. It seamlessly integrates with development tools, providing interactive training, customizable settings, and a focus on preventing vulnerabilities. This platform is ideal for enhancing coding standards and security awareness, training both new and existing developers through real-life context and continuous skill development.

## What are Codebashing's key features?

- Real-life remediation training: Simulates actual scenarios to build practical knowledge.
- Tournament feature: Facilitates competitions to sharpen skills competitively.
- Adaptive learning paths: Tailors content for compliance requirements.
- Early vulnerability discovery: Identifies issues before they manifest in live environments.
- Gamification: Engages users with interactive learning methodologies.
- Seamless integration: Easily embeds into existing development processes.

## What should you consider in user reviews?

- Improved coding habits: Fosters a culture of security-first coding practices.
- Knowledge transfer: Ensures that critical security techniques are effectively imparted.
- Skill development: Enhances developers' ability to spot and mitigate flaws early.
- User-friendly design: Ensures a straightforward and engaging learning experience.

Codebashing is increasingly being implemented in industries where secure code development is critical, such as finance, healthcare, and technology. Firms utilize it to train developers and security teams, integrate it within CI pipelines for continuous feedback, and leverage its tools to test and fortify software before deployment. It aids companies in building robust applications by embedding security training directly within their development workflows.

# Valuable Features

Excerpts from real customer reviews on PeerSpot:



“With Codebashing we can see a clear difference; the vulnerability fixing ratio became 160% per month, and the density counts started reducing after implementation.”



**Tharindu Malwenna**

Senior Application Security Engineer at a newspaper with 5,001-10,000 employees



“The kind of remediation that Codebashing trains developers on is outstanding, as it relates developers to real-life use cases.”



**AkashSingh**

Senior Product Specialist at Meteonic Innovation Pvt. Ltd.



“Codebashing has been supremely helpful in educating engineers and cybersecurity professionals within my team on how to practice secure coding.”



**Verified user**

DevSecOps Security Engineer at a manufacturing company with 10,001+ employees

- ✓ “In my opinion, the best features Codebashing offers are early vulnerability discovery, improved defensive coding habits, and catching what automated tests miss.”



**Verified user**

Lead Software Test Engineer at a tech vendor with 10,001+ employees

- ✓ “The installation phase of the tool is simple.”



**AnanyaRoy**

Risk Analyst at Deloitte

- ✓ “The platform is simple, easy to use, and easy to learn.”



**Taniya Roy**

I. T. Analyst at Tata Consultancy

- ✓ “The most important aspect of Codebashing, in my opinion, is the gamification advantage. When compared to competitors' offerings, the most significant thing to emphasize is gamification. The rest is similar to the competitors.”



**Cuneyt KALPAKOGLU Phd.**

Founder & Chairman at Endpoint-labs Cyber Security R&D

What users had to say about valuable features:

“The most valuable feature is that you get the security from the design of the training. It ensures our developers write code securely and effectively. They will not write code that is vulnerable to hackers..”

**Verified user**

[Read full review](#) 

System Engineer at a manufacturing company with 5,001-10,000 employees

---

“The platform is simple, easy to use, and easy to learn. It has comprehensive guidelines and a lot of documents and videos for an easy installation process. Apart from some default rules, it allows users to configure their own rules. Also, it is easy to configure as it has an extensive library for reference..”

**Taniya Roy**

[Read full review](#) 

I. T. Analyst at Tata Consultancy

---

“The most valuable features of the solution stem from the fact that its gamification UI is quite user-friendly to use, and it is also quite intuitive since it provides users with proper explanations while allowing one to opt for the obash option. Mapping is also quite accurate, which helps identify why the tool has flagged certain code or lines of code, making it helpful for users because sometimes you might be unable to detect the flaws on your own..”

**AnanyaRoy**

Risk Analyst at Deloitte

[Read full review](#) 

---

“In my opinion, the best features Codebashing offers are early vulnerability discovery, improved defensive coding habits, and catching what automated tests miss.

When I talk about early vulnerability discovery through Codebashing, I mean conducting intentional adversarial review very early during development or code review only, rather than waiting for QA, a pen test, or production incidents.

Additional features worth highlighting are shared security ownership, knowledge transfer across the team, common attacking patterns, how real-world exploits work, and better PR and design discussions since I started using Codebashing..”

**Verified user**

Lead Software Test Engineer at a tech vendor with 10,001+ employees

[Read full review](#) 

“The best features Codebashing offers include its interactivity, as it walks you through how the SQL injection exploit can happen while providing real-time feedback on what exact changes you need to make in your code to prevent it. This makes it a technology-agnostic approach, but also allows you to select which technology you write code in, providing specific examples relevant to your technology. For example, it shows how to perform input validation in Python to prevent a vulnerability such as SQL injection.

“Codebashing positively impacts our organization by improving awareness. We encourage product teams to have security ambassadors and use Codebashing to educate themselves on secure coding practices. While there is not a precise metric or KPI I can share on improving security posture, the overall awareness of these vulnerabilities is something that Codebashing helps strengthen..”

**Verified user**

[Read full review](#) 

DevSecOps Security Engineer at a manufacturing company with 10,001+ employees

---

“The kind of remediation that Codebashing trains developers on is outstanding, as it relates developers to real-life use cases.

I would like to highlight the tournament feature of Codebashing as great, allowing us to organize competitions among skilled developers, which helps identify the best and most productive individuals in our organization.

Codebashing's adaptive learning paths help us by addressing different use cases among our customers, as some follow OWASP Top 10 guidelines while others adhere to CWE, PCI DSS, or HIPAA. This means Codebashing helps us comply with these requirements so developers do not make mistakes when remediating issues found in the source code.

I have a very clear example regarding the measurable impact Codebashing has had on our team's ability to identify security flaws early in development. One customer in the aviation sector had around 7.8 vulnerabilities in one thousand lines of code before implementing Checkmarx or Codebashing. After using Codebashing, we improved our mean time to remediation (MTTR) and reduced the defect count to 3.6 in one thousand lines of code..”

**AkashSingh**

Senior Product Specialist at Meteonic Innovation Pvt. Ltd.

[Read full review](#) 

# Other Solutions Considered

“The reason I switched to Codebashing is that we were already a user of Checkmarx, and since Codebashing is a module of it, we got great pricing from the Checkmarx team, which is why we onboarded Codebashing as a fully-fledged tool..”

**AkashSingh**

Senior Product Specialist at Meteoric Innovation Pvt. Ltd.

[Read full review](#) 

---

“Based on the coverage we receive when comparing it with the IAS tool and the options we receive, such as ID integrations and direct impact on pull push requests, the pricing is much lower than IAS..”

**Tharindu Malwenna**

Senior Application Security Engineer at a newspaper with 5,001-10,000 employees

[Read full review](#) 

“It's my understanding that the company used to use SonarQube.

SonarQube starts right from the IDE and it has a MiFi interface. When the developer is developing they get to see the vulnerabilities from their IDE..”

**Dodzi Kwame Agudogo**

Senior Software Development Engineer at Stanbic Bank Ghana

[Read full review](#) 

---

“We are representing Checkmarx, and I am extremely familiar with Checkmarx, and Codebashing. I am well knowledgeable about all of these topics. I am familiar with them.

We are only working with Codebashing. Only with Codebashing. We are not that type of company. We are loyal to Checkmarx. On the other hand, there are not many similar products on the market..”

**Cuneyt KALPAKOGLU Phd.**

Founder & Chairman at Endpoint-labs Cyber Security R&D

[Read full review](#) 

“I have experience with AppScan and RiskSense. I was using AppScan to support DAST and RiskSense for getting results from SAST and DAST to generate reports. I was using different solutions for different reasons, but I think they provide different benefits to users. My company chose CheckMarx over AppScan since the former offers better source code scanning capabilities..”

**AnanyaRoy**

Risk Analyst at Deloitte

[Read full review](#) 

# ROI

Real user quotes about their ROI:

“With Codebashing we can see a clear difference; the vulnerability fixing ratio became 160% per month, and the density counts started reducing after implementation..”

**Tharindu Malwenna**

Senior Application Security Engineer at a newspaper with 5,001-10,000 employees

[Read full review](#) 

“I have not seen any quantitative return on investment metrics, but I can share that Codebashing has been supremely helpful in educating engineers and cybersecurity professionals within my team on how to practice secure coding..”

**Verified user**

DevSecOps Security Engineer at a manufacturing company with 10,001+ employees

[Read full review](#) 

“The return on investment will be one year.

I believe the product is valuable because it assists you in improving secure applications, which can then prevent fraud and threats against the application as well as incorrect application activities..”

**Peter Ejiofor**

Chief Executive Officer at Ethnos ITSolutions

[Read full review](#) 

# Use Case

“I am a reseller.

Codebashing is a training tool. It's a training tool that helps users or developers detect their coding errors and correct them. Then Codebashing shows them how to improve and secure their development skills..”

**Peter Ejiofor**

Chief Executive Officer at Ethnos ITSolutions

[Read full review](#) 

---

“I use Codebashing for security-related testing and aggressive testing, and also to stress-check code to expose weaknesses.

Ours is an HRA benefits application, and I use Codebashing for security testing or exposing weaknesses by attacking the input and intentionally passing malicious input. Through Codebashing, I can identify the required vulnerability. This means security testing, and a few of my colleagues have also been using Codebashing..”

**Verified user**

Lead Software Test Engineer at a tech vendor with 10,001+ employees

[Read full review](#) 

“We are very seriously using Codebashing. For example, when we have new engineers in the company, it is company policy that they have to complete the Codebashing sessions. During the orientation and onboarding period, all the engineers of our company must complete the Codebashings sessions and many of our customers are doing the same.

We are strategic partners with Checkmarx and we are an internationally certified training center for Checkmarx and Codebashing..”

**Cuneyt KALPAKOGLU Phd.**

Founder & Chairman at Endpoint-labs Cyber Security R&D

[Read full review](#) 

---

“I have used SonarQube as a community product for static application security testing as well as quality gate checking for the organization. Now I have retired the community edition of SonarQube and I am currently working with Checkmarx for a proper solution.

“In my current license configuration, I have Codebashing, secret scanning, and SAST.

“Codebashing is solely purposed for training our developers regarding the vulnerabilities we have, and it has seamless integration within Checkmarx. I am running a security champions program which leverages Codebashing platform itself..”

**Tharindu Malwenna**

Senior Application Security Engineer at a newspaper with 5,001-10,000 employees

[Read full review](#) 

“Codebashing serves as our primary tool for learning and awareness purposes, as one of my team's responsibilities is to spread awareness on secure coding practices. Codebashing helps facilitate that mission.

“A specific example of how we've used Codebashing to spread secure coding awareness in our team involves SQL injection, which is one of the top 10 OWASP vulnerabilities. Codebashing provides a very thorough walk-through example that explains SQL injection and demonstrates how to use parameterized queries, structured queries, and perform input validation. This exemplifies how we use Codebashing to educate product teams on writing secure code.

“While we do not integrate Codebashing with our workflow, we use it to educate product teams about the different kinds of vulnerabilities, such as the OWASP Top 10 and the SANS Top 25. We encourage product teams and developers to use the tool and rank teams based on who scores better on these assessments..”

**Verified user**

[Read full review](#) 

DevSecOps Security Engineer at a manufacturing company with 10,001+ employees

---

“I have been working with Codebashing, which is one of the modules in Checkmarx. Checkmarx has different modules like Codebashing, SAST, DAST, and SCA, providing a complete AppSec platform that includes Codebashing.

Codebashing has been integrated with our IDEs like Jenkins, Visual Studio, and Eclipse. Whenever a developer identifies any kind of security-related vulnerabilities, they receive a lot of information from Codebashing, such as what exactly the vulnerability is, how it can be fixed, any games around that, and any videos related to those vulnerabilities. The developer watches these videos and learns how to fix those specific issues. Additionally, we organize tournaments to test developer capabilities in terms of how quickly they can identify and fix issues, and how effectively they handle those issues without creating new ones.

For Checkmarx, we are the customer, and we use this particular platform to service our customers..”

**AkashSingh**

Senior Product Specialist at Meteonix Innovation Pvt. 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.

“The initial setup process is easy. It takes little time to complete for new users as well. However, it might take time if the infrastructure still needs to be implemented..”

**Taniya Roy**

I. T. Analyst at Tata Consultancy

[Read full review](#) 

---

“The initial setup is extremely easy. You don't need anything. Even a child can use it very easily. You don't need to install anything, it is web-based. You can use it very easily..”

**Cuneyt KALPAKOGLU Phd.**

Founder & Chairman at Endpoint-labs Cyber Security R&D

[Read full review](#) 

“The initial setup is straightforward. That's all there is to it once you install the tool.

It does not require any maintenance. People are not required to do anything. It is straightforward..”

**Peter Ejiofor**

Chief Executive Officer at Ethnos ITSolutions

[Read full review](#) 

---

“It is a cloud service, you, don't need any setup.

Very simple to deploy.

You can do it quickly, effortlessly, and effectively.

It is simple to deploy and use..”

**Cuneyt KALPAKOGLU Phd.**

Founder & Chairman at Endpoint-labs Cyber Security R&D

[Read full review](#) 

“The installation phase of the tool is simple.

The tool's installation phase took around 45 minutes.

The tool's installation phase was carried out by a team of 17 people in my company who use Checkmarx.

The solution is deployed on the cloud..”

**AnanyaRoy**

Risk Analyst at Deloitte

[Read full review](#) 

---

“Codebashing and Checkmarx SAST are really easy to set up; it is a matter of figuring out the SSO configuration from our end. The rest of the things are currently using the SaaS solution provided by Checkmarx, so the initial setup phase is straightforward.

“Scanning the entire organization takes time, which was one of the challenges we faced during the initial phase. To overcome such issues, we had to write scripts as workarounds..”

**Tharindu Malwenna**

Senior Application Security Engineer at a newspaper with 5,001-10,000 employees

[Read full review](#) 

# Customer Service and Support

“I have not interacted with customer support, as we did not reach out specifically to Codebashing. We had a contract with Checkmarx, and I have no complaints on that side..”

## Verified user

DevSecOps Security Engineer at a manufacturing company with 10,001+ employees

[Read full review](#) 

“With Codebashing solution, we had a couple of complications, such as account configuration issues. Because we are currently in the initial stages, the support is really good, but we have to wait and see..”

## Tharindu Malwenna

Senior Application Security Engineer at a newspaper with 5,001-10,000 employees

[Read full review](#) 

“The solution's technical support is good. My company has been able to resolve issues related to the tool with the help of Codebashing's technical support team. I rate the technical support a seven or eight out of ten..”

## AnanyaRoy

Risk Analyst at Deloitte

[Read full review](#) 

“So far, I believe Checkmarx has provided very good technical responses in all areas of their solution. Their technical response is excellent. They will contact you once you have booked your ticket.

I would rate their technical support a four out of five..”

**Peter Ejiofor**

Chief Executive Officer at Ethnos ITSolutions

[Read full review](#) 

“To be honest, the product never requires any form of technical support.

If customers require technical support, we provide it in our country, but there is no requirement because it is only a learning suite. There is no need for technical support for these types of products..”

**Cuneyt KALPAKOGLU Phd.**

Founder & Chairman at Endpoint-labs Cyber Security R&D

[Read full review](#) 

“We often communicate with the technical support of Codebashing, as we have dedicated technical support for that.

My impression of their support is positive, as they are available on calls and emails, and they provide fast responses, abiding by the signed SLA for technical responses. I find them to be highly professional.

I would rate their support a nine out of ten.

We have not had any significant issues, as all L1 and L2 issues have been remediated immediately over calls, although some complicated issues take time to resolve due to R&D and engineering involvement. Overall, support from Checkmarx is good..”

**AkashSingh**

Senior Product Specialist at Meteonic Innovation Pvt. Ltd.

[Read full review](#) 

## Other Advice

“If using Codebashing for a big team of more than 10 developers, it is important to plan to ensure the training is effective.

I would rate this solution a nine out of ten. .”

### Verified user

System Engineer at a manufacturing company with 5,001-10,000 employees

[Read full review](#) 

---

“Sometimes, Codebashing provides reports with false positives. Thus, I advise others not to rely on the reports and to do a thorough analysis. They may require to change a few configurations. Configuring your own rules is better than going for a default configuration.

I rate it an eight out of ten..”

### Taniya Roy

I. T. Analyst at Tata Consultancy

[Read full review](#) 

“We measure increased awareness through participation rates, which have been improving as people use the tool more consistently, leading to friendly competition within the enterprise to see who can rank higher and how many puzzles of Codebashing they have completed.

“My advice to others looking into using Codebashing is to proceed with it, as it is a brilliant tool. I would rate this review a 9..”

**Verified user**

DevSecOps Security Engineer at a manufacturing company with 10,001+ employees

[Read full review](#) 

---

“The solution is easy to maintain.

I think Codebashing is a great tool to start with if you are just learning about application security. Codebashing has some good tutorials and a nice learning platform to learn about coding. Codebashing also has a more nice gamification UI, which is a good tool. Generally, I think it's quite a good tool for developers to get started and pick up skills.

I rate the overall solution an eight and a half to nine out of ten..”

**AnanyaRoy**

Risk Analyst at Deloitte

[Read full review](#) 

---

“For knowledge transfer or shared security ownership in my team, we ask questions such as 'What happens if this field is missing or tampered?' and 'Should this ID come from a token instead of a request?' Such PR reviews and knowledge transfers have been conducted with real-world examples, including real payloads

that break assumptions and actual vulnerable code.

My advice regarding Codebashing would be to be practical, culture-focused, and incremental, starting with the high-risk areas such as authentication and authorization, data access APIs, and payments. The approach should focus on breaking the code, not the people.

I would rate this product a seven out of ten..”

**Verified user**

Lead Software Test Engineer at a tech vendor with 10,001+ employees

[Read full review](#) 

---

“To be honest, this is a very well-designed product, with the most essential competitive advantage being, as previously stated, gamification.

It is very user-friendly, simple to use, and simple to understand. The course duration is excellent. Certainly not more than eight or ten minutes, which is critical. From the perspective of a developer or programmer, those types of individuals are unable to allocate their time for too long.

These are the benefits of the product, and I enjoy it.

We are the partner. We are more than a reseller. We are the representative of Checkmarx in our region.

I would rate Codebashing a nine out of ten..”

**Cuneyt KALPAKOGLU Phd.**

Founder & Chairman at Endpoint-labs Cyber Security R&D

[Read full review](#) 

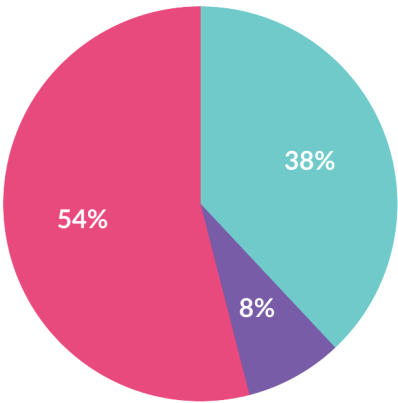
# Top Industries

by visitors reading reviews

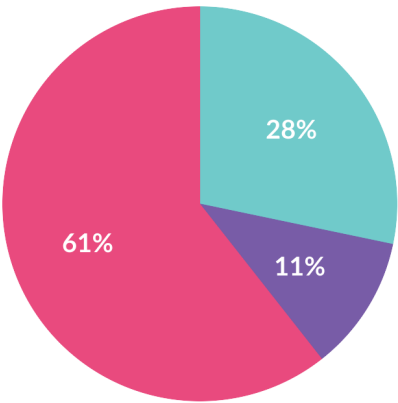


# Company Size

by reviewers



by visitors reading reviews



 Large Enterprise       Midsized 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](http://www.peerspot.com)

## PeerSpot

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

[reports@peerspot.com](mailto:reports@peerspot.com)

+1 646.328.1944