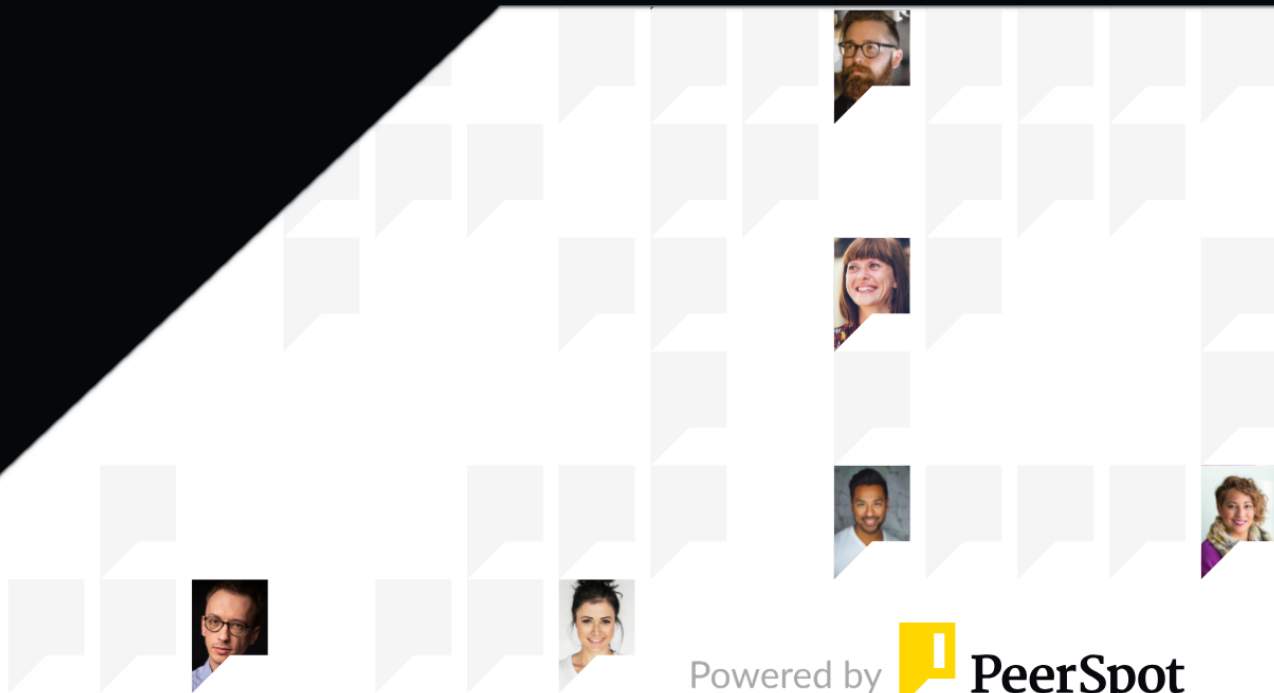


aws marketplace

Reco

# Reviews, tips, and advice from real users



Powered by  PeerSpot

# Contents

Product Recap..... 3 - 4

Valuable Features..... 5 - 8

Other Solutions Considered..... 9 - 10

ROI..... 11

Use Case..... 12 - 14

Setup..... 15

Customer Service and Support..... 16

Other Advice..... 17 - 18

Trends..... 19 - 20

About PeerSpot..... 21 - 22

# Product Recap



Reco

# Reco Recap

Reco is a versatile platform designed to optimize business processes by providing valuable data insights and streamlined communication. It offers actionable analytics that enhance decision-making capabilities.

Built for efficiency, Reco combines robust analytics with seamless communication tools to transform how businesses operate. It captures vital information, simplifying the process of turning data into actionable insights. By integrating advanced technology, Reco helps organizations enhance productivity and innovation.

## What are the most important features of Reco?

- **Actionable Analytics:** Delivers deep insights to inform strategic decisions.
- **Seamless Collaboration:** Facilitates communication to improve teamwork.
- **Customizable Dashboards:** Tailors information displays for user needs.
- **Real-Time Data Processing:** Ensures information is always up-to-date.

## What benefits should users look for in reviews?

- **Increased Efficiency:** Streamlines workflow, saving time and resources.
- **Enhanced Decision-Making:** Provides precise data for informed choices.
- **Cost Reduction:** Identifies areas for budget optimization.
- **Improved Team Collaboration:** Boosts teamwork through better communication tools.

Reco has a strong presence in sectors such as healthcare, finance, and retail, being tailored to meet industry-specific demands. In healthcare, it aids in patient management and data security, while in finance, it boosts risk assessment and compliance. For retail, Reco enhances customer insights and inventory control.

# Valuable Features

Excerpts from real customer reviews on PeerSpot:



“What I like about Reco is that it's pretty easy to integrate with the applications; it's almost plug and play.”



**Validated user**

Gerente De Arquitectura De Ciberseguridad at a financial services firm with 5,001-10,000 employees



“What I appreciated most about Reco was its strong detection capability.”



**Sharon Lawrence**

Ai Implementation, Consultant & Educator | Ai Product Manager at a media company with 5,001-10,000 employees



“We have seen a positive return on investment, estimating that the initial investigation effort has dropped by roughly fifty percent.”



**Ayush Pandey**

Digital solutions architect at a educational organization with 51-200 employees

## What users had to say about valuable features:

“What I appreciated most about Reco was its strong detection capability. It detected when we received a large volume of critical alerts and displayed those at the top, alerting us that it was urgent to investigate them..”

### Sharon Lawrence

Ai Implementation, Consultant & Educator | Ai Product Manager at a media company with 5,001-10,000 employees

[Read full review](#) 

---

“What I like about Reco is that it's pretty easy to integrate with the applications; it's almost plug and play. The interface and the user experience of the interface are very good, and it's very easy to find the detections, alerts, to filter, and to navigate the interface. The support is also very good; I have been implementing the solution with them, and they have been helping me a lot. The support works well, and it's also very good at prioritizing the detections, so I don't see many false positives.

“The key benefits that I have seen from using Reco are that it helps me to mitigate risks in SaaS applications; I have a lot of SaaS applications with many configurations inside. Without Reco, I am losing critical information to understand if I have risks in the cloud, so with Reco, I now have visibility. I am maybe not 100% sure, but in a high percentage, I can assure that I don't have high or critical risks in my SaaS applications, which are growing every day and becoming more important. It helped me to mitigate those risks, basically.

“The coverage of SaaS applications is very good; they cover almost all of my SaaS applications, and they have a big list of SaaS applications supported..”

### Validated user

Gerente De Arquitectura De Ciberseguridad at a financial services firm with 5,001-10,000 employees

[Read full review](#) 

“The best features that Reco offers, in my opinion, are the centralized view of the SaaS applications being used across our organization. For example, if a new SaaS application starts being used by an employee, Reco helps us identify it and investigate things such as who is using it, how widely it is being used, and whether it needs to be reviewed from a security perspective. This is particularly useful because manually tracking every application across a growing organization would be time-consuming. We also use the visibility to prioritize applications or users that require attention rather than manually reviewing everything. For us, the biggest value is having centralized SaaS visibility combined with security context, which helps us reduce manual investigations and gives our security team a better understanding of our SaaS environment.

“I had one incident approximately six months ago when our security team noticed that a new SaaS application, such as a project management or AI productivity tool, was being used by an employee. Previously, to investigate it, we might have had to check our identity providers to see which employees have access, look at application logs to understand usage, check with the application owner, and then manually determine whether the application should be approved. With Reco, we can start from a centralized view and quickly understand the application, who is using it, how broadly it is being used, and what security information is available around it. Instead of spending thirty or forty-five minutes collecting information from several places, we get the initial context much faster and focus on deciding whether there is an actual risk. I think this is the biggest time saving for us. It is not just that Reco puts information on one screen; it reduces the back and forth between different tools and teams during an investigation.

“Whenever I use Reco, I feel safe. Governance and security are definitely important considerations, especially because SaaS environments can contain sensitive organizational user data. Understanding what data is being processed is crucial.

“The breadth of coverage Reco offers for SaaS operations is strong, particularly around SaaS visibility, application discovery, and user and access context. Reco is not just showing us a list of applications; it gives us additional context that helps us understand how those applications are being used and where we may need to

investigate further. For example, identifying applications across the organization to understand associated users and access helps prioritize potential security or governance issues, which becomes particularly valuable as our SaaS environment grows.

“The use of eight different sensors for SaaS application discovery has made a noticeable difference for us. The main benefit is that we are not relying on a single source of information to discover SaaS applications, as different applications can show up through different signals, giving us broader coverage and making the discovery process more reliable. Having multiple sensors feed into Reco and provides a more complete picture of what is actually being used in the organization, reducing blind spots and the amount of manual discovery work for our team.

“The LLM integration is interesting because the knowledge graph gives context about the relationships between users, application access, and security signals. Instead of an analyst manually connecting those dots, the AI can help explain what is happening and why something might deserve attention, significantly speeding up investigation. This is probably the biggest differentiator compared with more traditional SaaS visibility tools.

“The AI agent security capability is particularly useful because AI agents are becoming another category of SaaS technology users that security teams need to understand. The biggest challenge is that agents can be connected to applications, APIs, and data sources, and sometimes have permissions to take actions on behalf of users. Discovering those connected AI agents and bringing them into the same governance process as the rest of our SaaS is quite valuable because we need to understand what is connected to what permission it has, what data it can access, and who owns it.

“My impression of Reco's Device Management feature when it comes to discovering every device in our organization is quite positive, particularly from a visibility perspective. One of the challenges with device management is getting a complete and up-to-date picture of what devices are present. Reco provides centralized device visibility without maintaining separate inventories and correlating devices with users and SaaS applications manually..”

# Other Solutions Considered

“We used alternatives such as Gurukul, which allows you to see malicious things triggering on a network basis instead of just the software, and we also had CrowdStrike. Those are a few alternatives we used..”

## Sharon Lawrence

Ai Implementation, Consultant & Educator | Ai Product Manager at a media company with 5,001-10,000 employees

[Read full review](#) 

---

“Before using Reco, we were actually using a combination of existing identity and security tools. The main limitation was that the information was fragmented, so we could not get a complete picture from different tools, which forced us to rely on a mix of Wiz, Okta, Zscaler, and Microsoft Defender..”

## Ayush Pandey

Digital solutions architect at a educational organization with 51-200 employees

[Read full review](#) 

“We evaluated several options before choosing Reco, which included comparing solutions such as Wiz, Netscope, Microsoft Defender, and assessing what we could have accomplished with our existing tools. Ultimately, we compared how well each solution could provide complete SaaS visibility..”

**Ayush Pandey**

Digital solutions architect at a educational organization with 51-200 employees

[Read full review](#) 

---

“I evaluated a couple of other options; I decided to go with Reco mostly because of the integrations, the supported integrations, and the user experience. How it shows the detections is pretty clear and organized, while the others either didn't integrate with some of my SaaS applications or they showed the posture detections very confusingly or were missing detections..”

**Validated user**

Gerente De Arquitectura De Ciberseguridad at a financial services firm with 5,001-10,000 employees

[Read full review](#) 

# ROI

Real user quotes about their ROI:

“We have seen a positive return on investment, estimating that the initial investigation effort has dropped by roughly fifty percent. Something that previously took thirty to forty minutes might now take fifteen to twenty minutes, providing the biggest measurable efficiency gain by saving twenty to forty hours of team time to focus on something more complex or prioritized..”

**Ayush Pandey**

Digital solutions architect at a educational organization with 51-200 employees

[Read full review](#) 

---

“It's difficult to find return on investment with Reco because it's more related to risk, to risk mitigation. I could say that maybe I have mitigated a couple of risks that could lead to money loss, but to be honest, I can't calculate that. Before Reco, I didn't have visibility on the posture of SaaS applications; it wasn't that I saved time with Reco; it was having more visibility and mitigating more risk, which is difficult to show as a return on investment..”

**Validated user**

Gerente De Arquitectura De Ciberseguridad at a financial services firm with 5,001-10,000 employees

[Read full review](#) 

# Use Case

“I used Reco when I worked at the company as a software security tool that monitored all the software the company was using. Reco functioned as a detection tool that identified any type of malicious event occurring within the software environment for users..”

## Sharon Lawrence

Ai Implementation, Consultant & Educator | Ai Product Manager at a media company with 5,001-10,000 employees

---

[Read full review](#) 

“My main use case for Reco is that it has been a valuable part of our security and SaaS visibility stack. Over time, I have found its main value to be giving us better visibility into our SaaS environment and helping identify areas that require attention. Reco is relatively straightforward to work with, and its centralized view makes it easier to investigate issues compared with checking individual applications manually.

“A specific example of how I used Reco to solve a problem and improve my workflow is when we were trying to understand an unfamiliar SaaS application in our environment. Instead of manually going through different systems to figure out who is using it and whether it needs attention, Reco gives a centralized place to start that investigation, which saves quite a bit of time, especially when dealing with a growing number of applications. For me, it is primarily the visibility that matters.

“I think another benefit is the context around the visibility because it helps us decide which findings actually need attention, rather than treating everything the same..”

**Ayush Pandey**

Digital solutions architect at a educational organization with 51-200 employees

---

[Read full review](#) 

“I implemented Reco for cybersecurity posture management for SaaS applications, and also for AI agents posture, so SaaS security posture management and agent posture management. I am using Reco for detecting attacks and generating alerts on bad behavior in SaaS applications, not only posture.

“I am using the eight different sensors for SaaS application discovery in my environment, and it works well. To be honest, I am not using that in depth, the discovery module; I know the SaaS applications that I have and I integrate them directly. I see that it's discovering applications through these sensors, and I am using the email one, which works well; it checks on the emails and sees if someone is using a SaaS application. But besides that one, I am not using the other sensors. That sensor is working well, but I am not, let's say, taking advantage of that module yet, the discovery module.

“My impression of Reco's AI Agent Security features ability to discover and govern connected AI agents is that it works well; I am using that for my agents on Copilot Studio. I integrate Reco with Copilot Studio, and it's showing me the agents, the inventory of agents, and the posture of those agents. It's working well, but the only problem was with the integration with Copilot Studio because there was a centralized integration; I have to integrate with each environment in Copilot Studio, so it's not easy to integrate because I have to go one by one, one agent per agent. But once I am integrated, it's very good; it shows good information and posture risks on those agents, so it's working well.

“I am aware of the pricing aspect of Reco.

“I am not using Reco's agents for automating tasks in my business processes.

“I do not use the device management feature in Reco..”

**Validated user**[Read full review](#) 

Gerente De Arquitectura De Ciberseguridad at a financial services firm with 5,001-10,000 employees

# 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 deployment process was pretty smooth; they were with me, the support helped me to deploy the solution, and they sent me all the step-by-step procedures for integrating with the SaaS applications. It was pretty smooth, and I didn't have any challenges there; the only challenge was the Copilot Studio integration that I had to do for each Copilot Studio environment..”

## Validated user

[Read full review](#) 

Gerente De Arquitectura De Ciberseguridad at a financial services firm with 5,001-10,000 employees

---

“Setting up Reco agents for automating tasks in our business processes is relatively straightforward, especially once the integrations and permissions are already in place. An agent could detect a SaaS application that meets certain risk criteria and then automatically notify the user owner or initiate a security review. The main thing we focus on is permission and guardrails for higher impact actions, wanting approval and auditability rather than giving the agent complete autonomy..”

## Ayush Pandey

[Read full review](#) 

Digital solutions architect at a educational organization with 51-200 employees

# Customer Service and Support

“I did not have to contact Reco's customer support because the client took care of that issue, but we did have team meetings with Reco sometimes. Sometimes we discussed any problems and concerns we had during live Reco tech support calls..”

## Sharon Lawrence

Ai Implementation, Consultant & Educator | Ai Product Manager at a media company with 5,001-10,000 employees

[Read full review](#) 

“The support is very good; I have been implementing the solution with them, and they have been helping me a lot. The support works well, and it's also very good at prioritizing the detections, so I don't see many false positives.

“I would evaluate customer service and technical support from Reco as very good..”

## Validated user

Gerente De Arquitectura De Ciberseguridad at a financial services firm with 5,001-10,000 employees

[Read full review](#) 

## Other Advice

“Reco is spelled R E C O. If Reco had a system for setting up agents to automate tasks in our business processes, that would be beneficial and would make things go much faster. Regarding Reco's use of eight different sensors for SaaS application discovery in our environment, I do not understand what they mean by that. I would rate this review a 7..”

---

**Sharon Lawrence**

Ai Implementation, Consultant & Educator | Ai Product Manager at a media company with 5,001-10,000 employees

[Read full review](#) 

“I am using Reco as a full SaaS.

“The only disadvantage at that moment was that Reco wasn't so popular; it wasn't implemented in companies in my region, so that was the only risk; it was a new tool without experience in at least companies that I could ask for recommendations.

“Based on my experience with Reco, I would say to test it, try it out, and see if it solves your problems. I have no advice to give except that it's a good product that has improved a lot over time. I would rate this review as a 9..”

---

**Validated user**

Gerente De Arquitectura De Ciberseguridad at a financial services firm with 5,001-10,000 employees

[Read full review](#) 

“Reco is not deployed in a completely private cloud environment for my organization. The cloud provider we use with Reco is [Google Cloud](#) Platform, or

[GCP](#). I did not find any much deviations since our organization is a long-term user of this Google Cloud provider, and most of the services are from Google Cloud, which we trust.

“My advice for others looking into using Reco is to consider that we evaluated a few alternatives before selecting it, focusing on SaaS discovery, visibility into users and access, security context, and the potential to eliminate manual investigations, which is why Reco stood out with its centralized view across different signals.

“I would rate Reco around eight out of ten. I choose this rating because of the improvements I am expecting, particularly more automations and customizations. The majority of things are correct, but I think in this AI era, everything is automated, and those two things would significantly reduce time. Regarding how Reco is deployed in my organization, I took the plan..”

**Ayush Pandey**

Digital solutions architect at a educational organization with 51-200 employees

[Read full review](#) 

# Top Industries

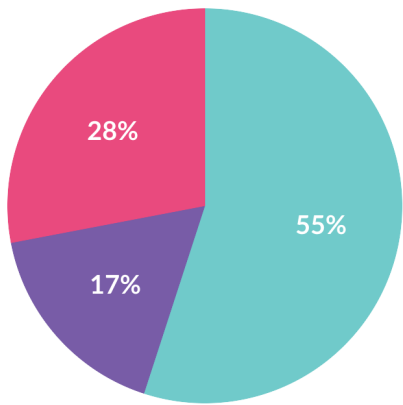
by visitors reading reviews



# 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](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