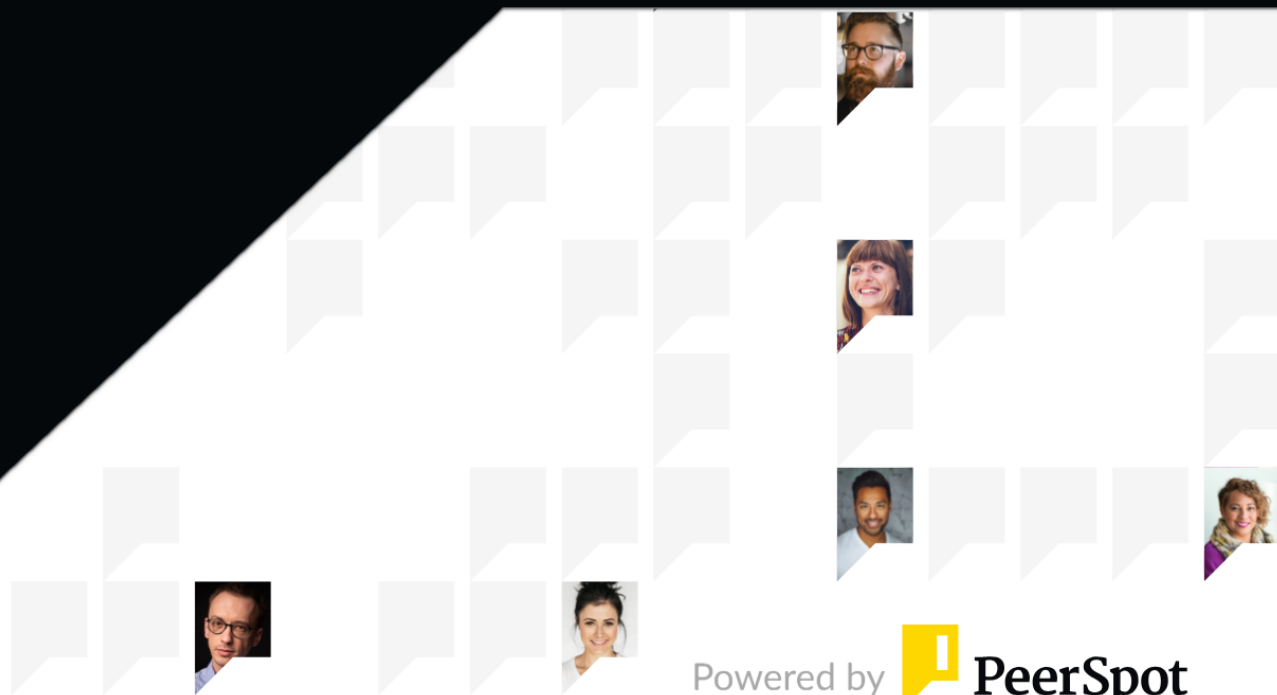


aws marketplace

Swimlane

Reviews, tips, and advice from real users



Powered by  PeerSpot

Contents

Product Recap..... 3 - 4

Valuable Features..... 5 - 10

Other Solutions Considered..... 11 - 12

ROI..... 13

Use Case..... 14 - 17

Setup..... 18 - 20

Customer Service and Support..... 21 - 22

Other Advice..... 23 - 26

Trends..... 27 - 28

About PeerSpot..... 29 - 30

Product Recap



Swimlane

Swimlane Recap

Swimlane provides a centralized platform for security orchestration, automation, and response. It enhances operational efficiency and reduces workloads through drag-and-drop task automation and integration capabilities.

Swimlane empowers IT teams by streamlining tasks with minimal coding, offering extensive customization, and enabling efficient incident response. Its features include centralized logging, visual workflow representation, and integration with third-party tools. Swimlane's task persistence and case management improve operational control but face issues with stability and latency. While marketed as a no-code platform, setup complexity requires skilled developers. Enhancing search, AI, and scalability is vital for improved usage in multinational environments.

What are Swimlane's essential features?

- **Centralized Log Portal:** Provides a unified view of logs improving monitoring.
- **Drag-and-Drop Design:** Facilitates workflow creation with minimal coding.
- **Integrations:** Seamlessly connects with third-party tools.
- **Visual Workflow:** Allows clear representation of processes.
- **Customizable Dashboards:** Enables tailored data visualization.

What benefits and ROI can users expect?

- **Operational Efficiency:** Saves time by automating repetitive tasks.
- **Reduced Workload:** Distributes tasks across teams enhancing productivity.
- **Cost Savings:** Lowers operational costs through streamlined processes.
- **Incident Response:** Improves management with adaptable case features.

In industries like IT and security, Swimlane serves as a SOAR platform for incident management and enriched alert integration. It's used for designing customer journey architectures and task assignments in multinational environments, despite requiring improvements in its initial setup and orchestration.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- ✓ “Swimlane positively impacts my organization as it is a product company that provides cybersecurity automation, and with multiple releases we now have a product called Turbine where we can do the same thing in a more advanced way with agentic AI and the use of AI/ML capabilities.”



Saketkumar Kumar

Senior Engineer at a outsourcing company with 501-1,000 employees

- ✓ “Swimlane has positively impacted my organization by saving a lot of time, reducing all the manual work that the SOC used to do, and improving response times.”



Validated user

Security automation specialist at a comms service provider with 51-200 employees

- ✓ “On a scale of one to ten, this solution deserves a rating of nine.”



MoumitaDas

Software Engineer III at a financial services firm with 10,001+ employees



“We are using it for a SOAR platform at a Cyber Security company which is MSSP.”



Validated user

Cybersecurity Consultant at a media company with 1,001-5,000 employees



“Swimlane has had a positive impact on my organization because it has saved us time and, based on using it for one client, we have started to integrate it for the rest of the clients.”



Izan Ayllon

Operator technician at a tech services company with 10,001+ employees



“The biggest advantage of Swimlane for us is that it saves time, which in turn helps us in cost-saving.”



Validated user

Senior Manager, Cyber Security at a tech vendor with 1,001-5,000 employees



“Our primary goal was to reduce analyst time, and we have been successful in that.”



Sairam S

Associate at Deloitte

What users had to say about valuable features:

“It has not impacted our organization positively, as we are using it primarily as a ticketing system. Normally, there should be some AI platform to include it and add alert traffic or other functionality, but it currently serves just as a ticketing system, which is not perfect..”

Validated user

[Read full review](#) 

Cybersecurity Consultant at a media company with 1,001-5,000 employees

The best features that Swimlane offers are the integration with all the other tools, it is very easy to use and very intuitive. Swimlane provides a lot of information and a lot of fluency when doing things, and it is one of the tools that I have used that works the best.

I sense that Swimlane was integrated with Sentinel and maybe BMC Helix, with CrowdStrike as well, though I don't know what integrations it has in the background because we work for an external client. .”

Izan Ayllon

[Read full review](#) 

Operator technician at a tech services company with 10,001+ employees

“I appreciate the UI and the ease of usability that Swimlane offers. What stands out to me about the UI of Swimlane is how everything has a feature on the side that you can easily move around, which is quite convenient.

“Swimlane has positively impacted my organization by helping us quickly work on alerts and document them. From being able to quickly work on alerts and document them, I have seen improved response times and efficiency since we are able to work very easily using the amazing UI and the tool..”

Validated user

[Read full review](#) 

Critical Incident Response Center Analyst (Circulation) at a tech vendor with 10,001+ employees

“The best features Swimlane offers are the flexibility of writing your own Python code and the existing workflows with a marketplace for the most known workflows, which is great because you can quickly use workflows similar to those in other solutions.

“Swimlane has positively impacted my organization by saving a lot of time, reducing all the manual work that the SOC used to do, and improving response times. It saved about ten minutes for every alert that comes out, and we get hundreds of alerts, meaning it saved many hours every day..”

Validated user

[Read full review](#) 

Security automation specialist at a comms service provider with 51-200 employees

“We do utilize the analytics aspect in Swimlane, and we use their Hero AI module as well.

“We also use customizable dashboards in Swimlane because many clients, including CISOs, whom we manage need an executive-level view of what is happening over Swimlane. We create dashboards for them that provide proper information, such as how many alerts were created, what was the mean time to triage, and mean time to respond; we cover all these as KPI metrics in the executive dashboard.

“The biggest advantage of Swimlane for us is that it saves time, which in turn helps us in cost-saving..”

Validated user

[Read full review](#) 

Senior Manager, Cyber Security at a tech vendor with 1,001-5,000 employees

“Swimlane is a low-code security platform with most things having connectors and plugins available from the marketplace. You can directly download and configure them and use them instead of writing multiple lines of code; you can directly use the connectors and get your task automated.

“Regarding my experience using those plugins from the marketplace, you can download whatever the use case is. Based on the use case, you just download the connectors or plugins available, configure them, and once those configurations are complete, create a playbook, design the workflow, and you can directly use an expression for obtaining the desired result. You can create a record for the SOC analyst team, and they can work on specific records, and you can also create UI buttons for the SOC analyst team. You can design another playbook that will be linked with the button. The SOC analyst will have a view to work on the records and can reassign tasks with everything done from the UI. You just need to integrate the workflow with the button. For instance, you can send notifications via multiple endpoints such as Microsoft Teams or Slack. You can configure the Slack connectors, create a playbook workflow, and then the SOC analyst can click a button to have the workflow post messages to the Slack channel, integrating multiple APIs using connectors.

“Swimlane positively impacts my organization as it is a product company that provides cybersecurity automation. Initially, it was Swimlane, but with multiple releases, now we have a product called Turbine, where we can do the same thing in a more advanced way with agentic AI and the use of AI/ML capabilities..”

Saketkumar Kumar

[Read full review](#) 

Senior Engineer at a outsourcing company with 501-1,000 employees

Other Solutions Considered

“If we consider options outside of Appian, Java has many similar solutions, but within Appian, the task assignment capability is uniquely provided by Swimlane..”

MoumitaDas

Software Engineer III at a financial services firm with 10,001+ employees

[Read full review](#) 

Before using Swimlane, we used TheHive and the decision was made because when we started using Swimlane for a specific client, we realized that the operation was much simpler and it didn't freeze as much.

Izan Ayllon

Operator technician at a tech services company with 10,001+ employees

[Read full review](#) 

“I wasn't part of the initial evaluation process. Still, we had some evaluations of other SOAR solutions within our company after migrating to Swimlane..”

Sairam S

Associate at Deloitte

[Read full review](#) 

“We have recently seen new products such as Tines and Blink Ops coming into the market, where a person with a good knowledge of APIs and JSON format can manage the platform and create playbooks. Even a security analyst can create some playbooks on those platforms. However, on Swimlane, it's difficult for security analysts since they must mandatorily know Python to create the playbooks..”

Validated user

[Read full review](#) 

Senior Manager, Cyber Security at a tech vendor with 1,001-5,000 employees

“We decided to move to Swimlane and Palo Alto as our SOAR solutions, as they are the most promising solutions in the market and have received positive reviews from their current users. Additionally, the support they provide is excellent. We had extensive interaction with the Swimlane team for about three months before we decided to purchase the tool. They showed us all the needed features and provided us with direct access to their developers and engineers so that we could ask questions or discuss any use cases. They even gave us the opportunity to practice and test the tool for ourselves. This level of support and flexibility was a stark contrast to what we had experienced with Splunk Phantom, so we decided to go with Swimlane..”

Srikanth Nuthalapati

[Read full review](#) 

Software Engineering Manager at Deloitte

ROI

Real user quotes about their ROI:

“We have seen a return on investment; with the same number of engineers, we now handle double the number of customers, even with the new, larger customers requiring dedicated teams, thanks to the automation we implemented in Swimlane leading to the need for fewer employees..”

Validated user[Read full review](#) 

Security automation specialist at a comms service provider with 51-200 employees

“I have seen a return on investment with Swimlane. I generally worked on the automation side to develop playbooks and workflows. If a company uses Swimlane, the SOC analyst team typically handles multiple events such as true positives and false positives. If everything is automated, we can filter out false positives or true positives, allowing for UI customization where the SOC analysts can trigger notifications and actions with buttons to create another playbook or automate using cron jobs, saving time for the SOC analyst team..”

Saketkumar Kumar[Read full review](#) 

Senior Engineer at a outsourcing company with 501-1,000 employees

Use Case

“We are using it for a SOAR platform at a Cyber Security company which is MSSP. We are providing services to other companies, and we are utilizing it as a SOAR platform..”

Validated user

Cybersecurity Consultant at a media company with 1,001-5,000 employees

[Read full review](#) 

“My main use case for Swimlane is as a SOAR platform and for documentation. I use Swimlane for documentation by documenting all the alerts that we get and adding all of our documentation..”

Validated user

Critical Incident Response Center Analyst (Circulation) at a tech vendor with 10,001+ employees

[Read full review](#) 

The main use case for Swimlane in my organization is carrying out analysis of alerts coming from other sources and analyzing IPs, domains, URLs, and more observables.

For example, we receive an alert that a user has accessed a suspicious URL, and therefore, we perform an analysis of that URL and in Swimlane we document the analysis of our investigation. .”

Izan Ayllon

[Read full review](#) 

Operator technician at a tech services company with 10,001+ employees

“I have been using Swimlane for almost four years.

“There are multiple use cases for Swimlane. I have mainly worked on phishing triage, building use cases for customers, automating their use cases using playbooks, and designing workflows. The implementation was for case and incident management, and we also have vulnerability management.

“For phishing triage, we monitor a mailbox and as soon as any email arrives in the inbox folder, the workflow is triggered, and we grab all the details of that email. We parse it and then use VirusTotal for obtaining scores for the email, which is how phishing triage works in Swimlane..”

Saketkumar Kumar

[Read full review](#) 

Senior Engineer at a outsourcing company with 501-1,000 employees

“My main use case for Swimlane is security automation workflows, automating most of the daily SOC workflows, especially ticketing, alerting, and reporting.

“The main workflow I automated with Swimlane that helped my team was connecting our SIEM, which is mainly Splunk, to a ticketing system, specifically Jira, with Swimlane in the middle. It automatically gets alerts or notable use cases from the SIEM, processes them through Swimlane, and sends them to Jira, performing a lot of logic and automation, including DFIR and automatic response to specific threats that can be automated..”

Validated user

[Read full review](#) 

Security automation specialist at a comms service provider with 51-200 employees

“We are using Swimlane for automation purposes and security orchestration.

“We are using Swimlane's Playbook Automation. One of the major playbooks that we use in Swimlane is for phishing email automation, so whenever there is a phishing email delivered to a user inbox, Swimlane will automatically sandbox that.

“We integrate Swimlane with third-party tools such as CrowdStrike, VirusTotal, URL Proofpoint, and all other different tools we have, so that we get various enrichment of any alerts to make sure that the analyst doesn't spend much time doing manual tasks and gets all the information from the tools in the Swimlane console itself.

“We use the case management feature in Swimlane as well. This case management feature is helpful because, in security, we don't want our security incidents to be visible to end users. For example, if I am using ServiceNow, I have to impose many restrictions on the backend table to ensure that whatever incidents are created and written into that table are not available to any end users or other IT team members. We use case management for that purpose so that our security alerts are isolated and only the security team has visibility on them. Whenever we need any remediation, we integrate it with ServiceNow, so if I need to raise a remediation ticket for re-imaging the system, we can create a ticket in ServiceNow from the Swimlane console or from the case management itself with all the proper information..”

Validated user[Read full review](#) 

Senior Manager, Cyber Security at a tech vendor with 1,001-5,000 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.

I don't know how my experience has been with Swimlane's licensing costs, initial setup, and pricing model because that is not within my field of knowledge in the company.

Izan Ayllon

[Read full review](#) 

Operator technician at a tech services company with 10,001+ employees

The initial setup was straightforward due to Swimlane's customization capabilities. They provide standard solutions, but adjustments are needed based on requirements.

Validated user

[Read full review](#) 

Works

“The initial setup of Swimlane is easy to learn but requires customers to design their solutions. Deployment of Swimlane took us three to four months, which involved migrating existing playbooks..”

Sairam S

Associate at Deloitte

[Read full review](#) 

“The initial setup is complex because we have to connect to another SIEM. We are currently in the deployment stage for our customer and have not yet completed it. So far, we have been working on the deployment for about six months..”

Krisada Cheevamongkol

CEO at Nextwave(Thailand)

[Read full review](#) 

“Installation can be quite complex, especially when we have to use Kubernetes, and if we need to create load balancing. In those situations, it requires a good engineer to deploy the platform..”

Validated user

Senior Manager, Cyber Security at a tech vendor with 1,001-5,000 employees

[Read full review](#) 

“For the initial setup, the licensing needs to be handled appropriately. Existing applications wanting integration must have their process structures within Appian, as Swimlane isn't exposed. A process image is necessary in Appian to use Swimlane, which can be a drawback..”

MoumitaDas

[Read full review](#) 

Software Engineer III at a financial services firm with 10,001+ employees

Customer Service and Support

Customer service is commendable. When I raise a ticket, they reply within half an hour with an initial response, signifying that an agent has been assigned and is working on the issue.

Validated user

Works

[Read full review](#) 

“Customer support was very helpful and responsive; once I had a disaster, and they provided assistance within the same hour. I would rate customer support a ten..”

Validated user

Security automation specialist at a comms service provider with 51-200 employees

[Read full review](#) 

“Customer support is quite good, taking time for resolution but acknowledging within the timeframe and trying to resolve use cases as quickly as possible, including escalations to senior staff if needed..”

Saketkumar Kumar

Senior Engineer at a outsourcing company with 501-1,000 employees

[Read full review](#) 

“Appian community is there for technical support. You can raise a ticket or incident, and it gets addressed based on priority. Additionally, working with a firm that has a dedicated person for support is beneficial.

“If the primary support contact is unable to assist, tickets must be created within the Appian community, though sometimes response times extend for weeks..”

MoumitaDas

Software Engineer III at a financial services firm with 10,001+ employees

[Read full review](#) 

Other Advice

My advice to someone who is considering using Swimlane is that they try it before implementing it, and I would say that it is one of the leading tools currently. I gave this review a rating of 9.

Izan Ayllon

Operator technician at a tech services company with 10,001+ employees

[Read full review](#) 

“My advice for others considering using Swimlane is to ensure it is the right fit for you and to have someone capable of managing the [Kubernetes](#) cluster if you use it on-premises. If not, it is great to have it on the cloud, and you will definitely need people who understand Python for writing custom workflows. I would rate this solution a seven overall..”

Validated user

Security automation specialist at a comms service provider with 51-200 employees

[Read full review](#) 

“Swimlane is in the middle class range in terms of expense.

“I am not the decision maker, but I do not think it is worth the money to have as a tool.

“I would not recommend using Swimlane.

“On a scale of 1–10, I rate this solution a 5..”

Validated user

Cybersecurity Consultant at a media company with 1,001-5,000 employees

[Read full review](#) 

“On a scale of one to ten, I would rate Swimlane a nine. I chose nine because it is a pretty great tool and the only reason I did not give a full ten is because there is room for improvement and how it always should be.

“Regarding Swimlane's AI capabilities, I have not used it so I cannot say anything about its governance and security. I cannot say anything about the accuracy and reliability of output since I have not used it yet.

“My advice to others looking into using Swimlane is to keep an open mind; it might be a lot in the start, but it is an amazing tool. Give it some time, get used to it, get your hands dirty, and you will love this tool after a while. I have no additional thoughts about Swimlane, just keep improving, keep doing what you do, and you are doing a great job. My overall rating for Swimlane is nine out of ten..”

Validated user

Critical Incident Response Center Analyst (Circulation) at a tech vendor with 10,001+ employees

[Read full review](#) 

“The best part of Swimlane is the persistent notifications and its ease of integration, requiring minimal coding. While it lacks response features, it can be integrated with messaging or queue services to achieve this. Any incident response requires additional integration since Swimlane itself doesn't react to incidents.

“Real-time data in terms of persistence is configurable, and without config, tasks persist indefinitely until completion. If using Appian versions below 11, integration features for Swimlane aren't available. By default, Swimlane lacks built-in intelligence, needing coding for integration.

“Although the Swimlane is beneficial and reduces manpower requirements, it's hindered by its lack of exposure. If exposed through services or endpoints, its functionality could be accessed without needing a local standalone application.

“On a scale of one to ten, this solution deserves a rating of nine..”

MoumitaDas

Software Engineer III at a financial services firm with 10,001+ employees

[Read full review](#) 

“Swimlane offers this too, but it depends on the user's preference, similar to how some prefer Flipkart while others prefer Amazon. Since I worked with Swimlane, I felt more comfortable compared to Splunk.

“Regarding Swimlane's AI capabilities, I think we have pretty good security for credentials with [Bitwarden](#), which we promote for sharing all details. Additionally, there is an architect who designs the workflows or playbooks, and development will be done based on that, which is quite good.

“Regarding Swimlane's AI capabilities, its accuracy and reliability are quite good. I have worked with multiple APIs, and when we have the proper credentials, everything gets done on time, the accuracy remains high, and it takes less time. We compare response times of the APIs, and since we use plugins and connectors, it depends totally on the API response and the result from the API. Swimlane

automates the SOC analyst tasks.

“Swimane is quite good without needing any additional improvements.

“I would advise others to consider Swimlane as it is quite simple and user-friendly, with training provided for new customers or developers through good training materials, making it easy to learn for those unfamiliar with Swimlane. I would rate Swimlane around eight on a scale of one to ten.

“I feel that compared to other tools such as Splunk, which has other functionalities and was in the market before Swimlane, the reason for my rating is that Splunk provides more flexibility in writing code. You can have a custom code block to write Python scripts..”

Saketkumar Kumar

Senior Engineer at a outsourcing company with 501-1,000 employees

[Read full review](#) 

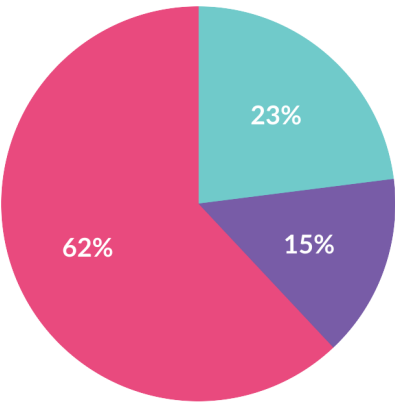
Top Industries

by visitors reading reviews

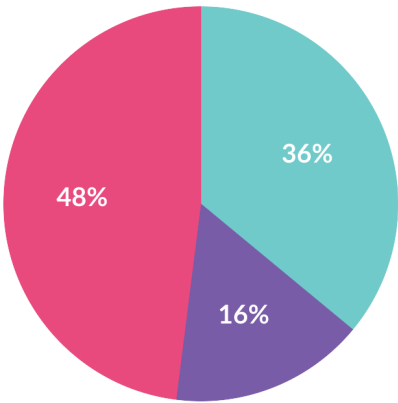


Company Size

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

PeerSpot

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

reports@peerspot.com

+1 646.328.1944