

aws marketplace

Sysdig Secure

# Reviews, tips, and advice from real users



Powered by  PeerSpot

# Contents

Product Recap..... 3 - 4

Valuable Features..... 5 - 9

Other Solutions Considered..... 10 - 11

ROI..... 12

Use Case..... 13 - 15

Setup..... 16 - 20

Customer Service and Support..... 21 - 23

Other Advice..... 24 - 26

Trends..... 27 - 28

About PeerSpot..... 29 - 30

# Product Recap

**sysdig**

Sysdig Secure

# Sysdig Secure Recap

In the cloud, every second counts. Attacks move at warp speed, and security teams must protect the business without slowing it down. Sysdig stops cloud attacks in real time, instantly detecting changes in risk with runtime insights, a unique AI architecture, and open source Falco. Sysdig delivers live visibility by correlating signals across cloud workloads, identities, and services to uncover hidden attack paths. By knowing what is running, teams can prioritize the vulnerabilities, misconfigurations, permissions, and threats that matter most. From prevention to defense, Sysdig helps enterprises move faster and focus on what matters: innovation.

*Sysdig. Secure Every Second.*

# Valuable Features

Excerpts from real customer reviews on PeerSpot:



“I have not seen any stability issues so far.”



**KS10**

Senior Presales Consultant at Techlab security



“The proactiveness of the support has been fantastic. Every time we mention something in a meeting that we're trying to do, he proactively takes that as an investigation topic and looks into it. He'll provide the solution even though we might not have asked him to investigate it.”



**Dan185638**

Global Information Security Officer at a tech services company with 51-200 employees



“The most valuable feature is the level of support that we get. Our solutions or customer success representative is very valuable. I see them as an extension of our security team.”



**Peter Du**

CISO at a recruiting/HR firm with 51-200 employees

- ✓ “The tool has the capability to conduct scans initially. It can perform scans on your virtual machines, physical machines, containers, and container images. A standout feature is its ability to scan offline container images stored in your container registry. Additionally, it can scan runtime images in your cluster or on your host machine. This allows for the detection of vulnerabilities in running containers, including loaded libraries. Notably, the tool can identify which library vulnerabilities are already present in your system. An added advantage is its capacity to take action beyond threat detection. It has the ability to block access and respond to encountered threats.”

**SunilKumar28**

DevOps Specialist at a manufacturing company with 10,001+ employees

- ✓ “We appreciate this feature, especially when combined with CD monitoring. The implementation of requested features has been remarkable, such as scanning for compliance in CRM processes for the US government. We heavily rely on this feature to assess compliance with federal requirements.”

**Mario Simko**

Observability team leader at SAP concour

- ✓ “Sysdig Secure has many strong foundational features like compliance and benchmark, security, network access management, and vulnerability management.”

**Burak AKCAGUN**

Business Development Manager at Axoft Ukraine



“The log monitor is the most valuable feature.”



**Verified user**

IT Manager at a tech services company with 201-500 employees

What users had to say about valuable features:

“The solution's runtime security and Falco are the two features I found to be the most valuable ones. So, Falco is their open-source tool for rules and policies..”

**Verified user**

Cybersecurity Sales Specialist at a outsourcing company with 51-200 employees

[Read full review](#)

---

A valuable feature of Sysdig Secure is that it is a pure-play vendor focusing on cloud-native protection. The product benefits from the Falco platform, developed by one of the founding members, which contributes to in-depth monitoring of cloud-native applications. It has strong detection and response capabilities that are more robust than other players, starting from posture management.

**KS10**

Senior Presales Consultant at Techlab security


[Read full review](#)

“Sysdig is user-friendly. Many other vendors we seriously considered had vast, complicated interfaces. Sysdig makes it quick and easy to do what you need to do. That's one thing I like about the platform, It takes you seconds to find what you want. There are not a lot of submenus or complex UI components.

The other valuable feature is runtime detection. The enhanced visibility they have within Kubernetes is longer than the workload. The visibility and the depth of information make a security professional's job a lot easier. It helps us sleep at night because we know that can get information about threats that we need when we need it. .”

**Dan185638**

Global Information Security Officer at a tech services company with 51-200 employees

[Read full review](#) 



“I see Sysdig as the most comprehensive solution in comparison to its competitors. For example, Sysdig can touch Cloud Security and allows you to add a user. I am a Sysdig user and it can be connected to Azure, AWS, or Google Cloud platform and they can gain visibility into the cloud. Also, Sysdig can touch so many areas of DevSecOps. For example, Sysdig Secure can inspect the Terraform Configs and also can be used for image scanning and benchmarking to your Kubernetes. Sysdig can regulate you to the SecOps of CIS..”

**Firat Y.**

Security Consultant at a tech services company with 1,001-5,000 employees

[Read full review](#) 

## Other Solutions Considered

“We previously used an open source solution. This is the first solution we have used for this kind of work. We are using syslog-ng with Sysdig, and I am comparing them both. .”

### Verified user

IT Manager at a tech services company with 201-500 employees

[Read full review](#) 

---

“We consistently explore new solutions through proof of concept to assess if there's anything that could potentially replace or offer superior features. Thus far, we haven't come across anything that comprehensively covers all the features Sysdig Secure has, while also maintaining the same level of support and documentation..”

### Mario Simko

Observability team leader at SAP concour

[Read full review](#) 

“In addition to Sysdig, we looked at Aqua Security, Palo Alto, Check Point, and Wiz. Check Point and Palo Alto had complicated interfaces like they had acquired and smashed other products into one interface. One of them was using Sysdigs open-source engine that they had implemented incorrectly, so we decided if others are using Sysdig's engine we might as well go to Sysdig to get the best experience.

We decided not to go with Wiz because it was more compliance-focused and didn't have much to offer in the container security space. We're more focused on container security than posture management and compliance. That was more like an add-on for us. Aqua was ridiculously expensive, and we didn't feel like we were getting more value than we would from Sysdig. .”

**Dan185638**

Global Information Security Officer at a tech services company with 51-200 employees

[Read full review](#) 

# ROI

Real user quotes about their ROI:

“We have definitely seen an ROI time-wise and resource-wise. I feel that I have an extension to our security team with this service. It gives us a lot of visibility that we would not have otherwise. It has saved 50% of an information security professional..”

**Peter Du**

CISO at a recruiting/HR firm with 51-200 employees

[Read full review](#) 

# Use Case

“We use Sysdig for cloud and Kubernetes posture management, including Kubernetes workload security, image vulnerabilities, and pipeline vulnerabilities. We use it across 2 of our cloud vendors: AWS and GCP..”

**Dan185638**

[Read full review](#) 

Global Information Security Officer at a tech services company with 51-200 employees

---

“I got the product for Dell SecOps. I am also interested in Kubernetes Stack and managed that product because it gives importance to the CI/CD pipeline security and most importantly the Falco Project. There are lots of big brands that contribute to Falco so I give importance to it. Moreover, Sysdig is also the founder of Wireshark and I think they are creating importance in the security area. .”

**Firat Y.**

[Read full review](#) 

Security Consultant at a tech services company with 1,001-5,000 employees

---

“We use Sysdig Secure to gain visibility into our runtime workloads. We use a whole bunch of security tools to scan our images before they get deployed into our production clusters. We needed a tool to give us runtime visibility and threat detection.

By implementing Sysdig Secure, we were trying to see any gaps. When an image is running, we wanted to see if any high or medium-scale vulnerabilities were picked up during the scanning and were running in a live workflow. We understood that we had a gap there. If there was a threat for us, we wanted to make sure that we knew and that we could scan our environment for any zero-day threats or vulnerabilities in general..”

**Peter Du**

CISO at a recruiting/HR firm with 51-200 employees

[Read full review](#) 

“The use case involves a robust security tool. We conducted evaluations of numerous tools to enhance our security measures. This assessment extended beyond just the systems. We also considered Falco, their open-source version, and Sysdig Falco Platform. Notably, the Falco Platform is integrated into the Sysdig Secure product. The central theme here is security in the context of Sysdig Secure. This tool offers security solutions for various domains including containerized platforms, virtual machines, VDI setups, and safeguarding code repositories like GitHub and Bitbucket. Furthermore, the tool provides insights that stand out distinctly from other products available today. Despite using Microsoft Defender for our virtual machines, it doesn't match up to the comprehensive outcomes delivered by Sysdig Secure. The tool furnishes detailed reports on aspects such as Intrusive Communication, thread level, process level, network level, specific ports, ingress and egress traffic, etc. This comprehensive vantage point empowers vigilant monitoring of all activities within the environment..”

**SunilKumar28**

[Read full review](#) 

DevOps Specialist at a manufacturing company with 10,001+ 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 solution was easy to deploy and easy to use. The technicians found that it was not too difficult to use.

The initial setup was not complex. It's easy..”

## Verified user

IT Manager at a tech services company with 201-500 employees

[Read full review](#) 

“It was extremely straightforward. We just installed the agent, and then we could see the dashboard light up. It took a few hours.

It is deployed on the cloud. The cloud deployment is at one location, but the agent is installed at multiple locations..”

## Peter Du

CISO at a recruiting/HR firm with 51-200 employees

[Read full review](#) 




“Initially, it was challenging. The documentation was insufficient, but over the years, there has been significant improvement. They now offer comprehensive, step-by-step documentation, including Helm Charts, making deployment, especially for those using Helm, quite straightforward in my opinion. We initially began with on-premises deployment but later transitioned to the cloud due to engineering resource constraints, finding it more manageable to handle.

The on-premises deployment took a few days, given its complexity. Now, deploying upgrades or similar tasks takes a maximum of two hours, including testing. .”

**Mario Simko**

Observability team leader at SAP concour

[Read full review](#) 

“I rate the solution's initial setup a six out of ten. So, one needs to have good and dedicated personnel or a team to ensure it is up and running.

Only one person is required if the deployment is being carried out for a small team. However, a handful of people would be required if the deployment is being carried out for an extensive team.

The deployment process typically involves various roles, including security engineers and cloud architects. These professionals may need to have visibility into the underlying STL stack to ensure a secure and efficient deployment..”

**Verified user**

[Read full review](#) 

Cybersecurity Sales Specialist at a outsourcing company with 51-200 employees

---

“The deployment is straightforward on the Sysdig side, but internal politics always make things difficult. The instructions to deploy are simple. It took less than an hour to deploy it across our entire environment. We have two cloud engineers responsible for deploying and maintaining it.

Like everything, Sysdig requires maintenance after deployment. I've been in tech for more than a decade, and we're always hoping for a product that we don't need to worry about after deployment. No matter what product it is, there's always maintenance to some degree, but it isn't a headache.

It comes down to proactive account management. Sysdig contacts us directly when they roll out updates. I'm happy to sit on the call and run through what needs to be done or any concerns. There is obviously some type of maintenance we need to do on the product over time. It isn't too difficult. .”

**Dan185638**

[Read full review](#) 

Global Information Security Officer at a tech services company with 51-200 employees

---

“The process isn't straightforward, as it involves setting up multiple components and deploying around six or seven parts. Handling this on-premises can be quite cumbersome. I wouldn't describe it as extremely complex, but it does carry a level of complexity. It was a long process as the configuration involved various internal aspects such as firewalls and URL access. This process took approximately a week, considering the need to establish the necessary access due to our on-premises setup.

We were particularly interested in deploying the solution on-premises due to our internal requirements. We were hesitant about opting for the SaaS platform due to data transfer concerns. However, an issue we encountered was that the on-premises version has a delay of six months compared to their SaaS offering. To address this, they proposed an alternative solution. If we have an AWS environment or a similar setup on our on-premises infrastructure, they can assist us in hosting the solution there. This introduces a distinct deployment model with three options: on-premises, SaaS, and a hybrid model that leverages our existing AWS setup.

.”

**SunilKumar28**

[Read full review](#) 

DevOps Specialist at a manufacturing company with 10,001+ employees

# Customer Service and Support

Customer support for Sysdig Secure could improve, especially in hiring more staff to cover different time zones and provide better coverage in the Asia Pacific region.

**KS10**

Senior Presales Consultant at Techlab security

[Read full review](#) 

---

“The technical support offered by the vendor is good. The technical support is very knowledgeable. I rate the technical support team an eight or nine out of ten..”

**Verified user**

Cybersecurity Sales Specialist at a outsourcing company with 51-200 employees

[Read full review](#) 

---

“I would rate their customer service an eight out of ten purely because I have it in a proactive manner. I meet our solutions engineer every fortnight, so I usually do not require support at all..”

**Peter Du**

CISO at a recruiting/HR firm with 51-200 employees

[Read full review](#) 

“They were well aware of our potential purchase, so their responsiveness was quite high. Even though the initial free trial was for thirty days, they essentially extended it to an unlimited timeframe. I can still access it, and it's functioning well. The process was swift, and we engaged in several support calls during that period..”

**SunilKumar28**

DevOps Specialist at a manufacturing company with 10,001+ employees

[Read full review](#) 

---

“We regularly reach out to them with any questions, even minor ones, as that's the support they offer us. I'm not sure if we're considered a valuable customer or if this level of support is standard for everyone, but they always encourage us to ask about anything. So, we frequently ask questions, even simple ones like constructing a proper query from their perspective, and they assist us with these tasks..”

**Mario Simko**

Observability team leader at SAP concour

[Read full review](#) 

“I rate Sysdig support 8 out of 10. We have an assigned Sysdig Solutions Architect who we meet with every 2 weeks. He goes above and beyond. He's extremely attentive to our tenancy and requirements. I get messages from him saying, "Oh, I've been working on this. Here's a solution to that thing you're talking about." or 'I've just checked these reports for you and found this.'"

The proactiveness of the support has been fantastic. Every time we mention something in a meeting that we're trying to do, he proactively takes that as an investigation topic and looks into it. He'll provide the solution even though we might not have asked him to investigate it. He's my main source of product support, but we also go through the service desk for more BAU requests and problems. .”

**Dan185638**

Global Information Security Officer at a tech services company with 51-200 employees

[Read full review](#) 

## Other Advice

Overall, I rate my experience with Sysdig Secure at 8.5 out of 10, closer to nine. Improvements could be made in support, scalability, and posture management.

**KS10**

Senior Presales Consultant at Techlab security

[Read full review](#) 

---

“I would offer the same advice to anyone considering a new product—always compare and weigh the pros and cons based on your specific use case. Overall, I would rate it 8 out of 10. .”

**Mario Simko**

Observability team leader at SAP concour

[Read full review](#) 

---

“I would tell those planning to use the solution that, from a container standpoint, it's excellent. If you're looking at it for other things, other vendors might be able to offer you better tools. Overall, I rate the solution an eight out of ten..”

**Verified user**

Cybersecurity Sales Specialist at a outsourcing company with 51-200 employees

[Read full review](#) 

---

“I compared Sysdig Secure with other solutions like Aqua by opening a demo trial



account and examining its features and benefits for one month.

Overall, I rate Sysdig Secure a nine out of ten..”

**Burak AKCAGUN**

Business Development Manager at Axoft Ukraine

[Read full review](#) 

---

“If you have the right approach to resolving vulnerabilities, it is an extremely useful tool. It is not useful if you plan to just have it deployed and not take action on any of the vulnerabilities.

I would rate Sysdig Secure a nine out of ten. If it has better reporting capabilities to visualize trends over time, it will be a more complete product..”

**Peter Du**

CISO at a recruiting/HR firm with 51-200 employees

[Read full review](#) 

“It hasn't necessarily freed up time for me. I haven't noted any time to value yet.

It's a good solution and better than the open source option I tested. I need more time to test and clarify the solution. While it is okay, I expect more from it. I'd like to have something that is out of the box.

I'd rate the solution an eight out of ten. .”

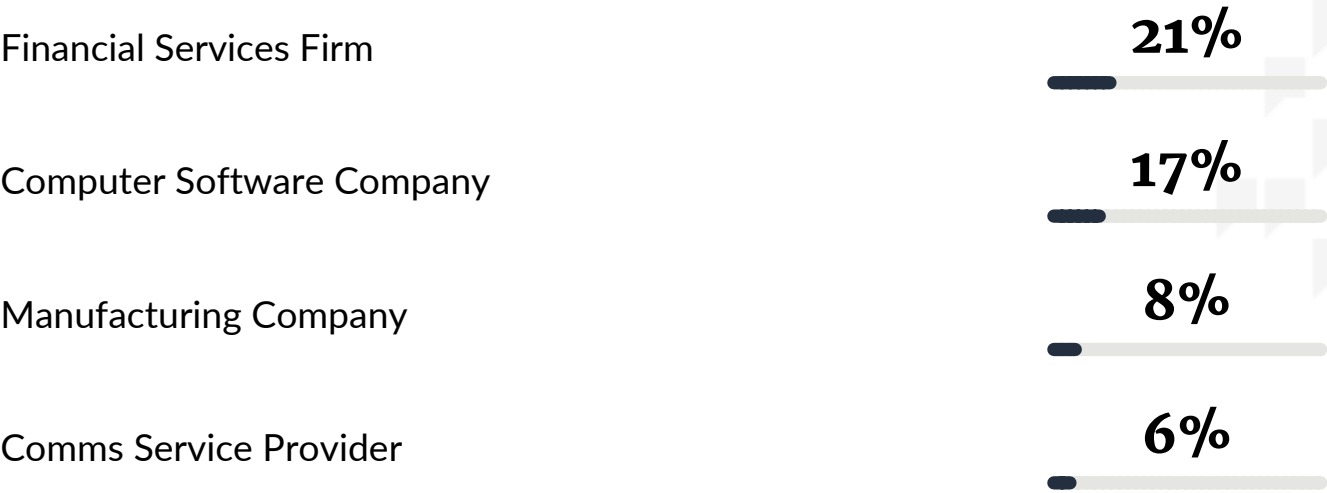
**Verified user**

IT Manager at a tech services company with 201-500 employees

[Read full review](#) 

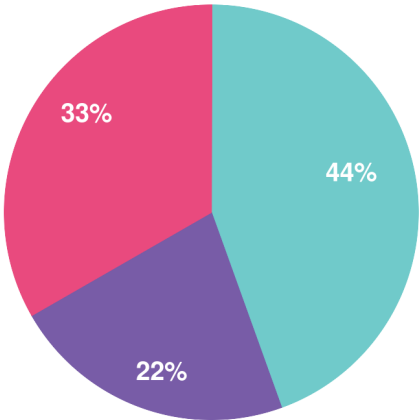
# Top Industries

by visitors reading reviews

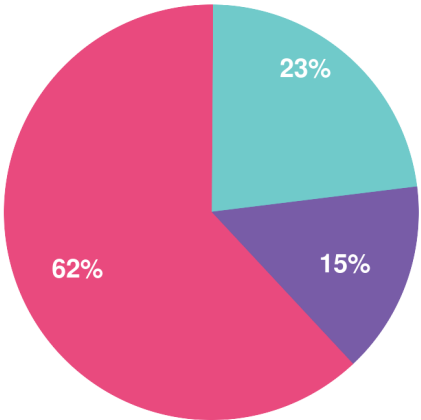


# Company Size

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 software running on AWS and other platforms. We created PeerSpot to provide a trusted platform to share information about software, applications, and services. Since 2012, over 22 million people have used PeerSpot to choose the right software for their business.

PeerSpot helps tech professionals by providing:

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

Use PeerSpot to:

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

Join PeerSpot to connect with peers to help you:

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

Visit PeerSpot: [www.peerspot.com](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