

aws marketplace

Skyhawk Security

Reviews, tips, and advice from real users



Powered by  PeerSpot



Contents

- Product Recap..... 3 - 4
- Valuable Features..... 5 - 11
- Other Solutions Considered..... 12
- ROI..... 13
- Use Case..... 14 - 16
- Setup..... 17
- Customer Service and Support..... 18
- Other Advice..... 19 - 22
- About PeerSpot..... 23 - 24

Product Recap



Skyhawk Security

Skyhawk Security Recap

Skyhawk Security provides advanced threat detection and response, offering businesses comprehensive cybersecurity management in an ever-evolving digital landscape.

Skyhawk Security stands out in threat intelligence, delivering robust solutions tailored to enhance cybersecurity protocols for organizations. It specializes in detecting and analyzing potential threats with high accuracy, effectively minimizing risks. Its intuitive technology allows for streamlined integration and efficient scalability, making it adaptable for businesses of different sizes and requirements.

What features does Skyhawk Security offer?

- **Advanced Threat Detection:** Identifies threats quickly and accurately, reducing potential risks.
- **Scalability:** Adapts to business size and growth without compromising performance.
- **Intuitive Integration:** Seamlessly integrates with existing systems for easier management.

What benefits should users look for?

- **Cost Efficiency:** Reduces the need for extensive manual security management, saving costs.
- **Improved Risk Management:** Enhances identification and response capabilities, lowering threat impacts.
- **Time Savings:** Automates routine tasks, allowing teams to focus on strategic security measures.

Industries such as finance, healthcare, and retail implement Skyhawk Security to strengthen their defenses against cyber threats, ensuring data protection and compliance with industry regulations. Its adaptable solutions provide the reliability needed in these sectors, offering peace of mind and robust security management.

Valuable Features

Excerpts from real customer reviews on PeerSpot:

- ✔ “Skyhawk Security has had a really positive impact on our organization, especially in reducing false positives and speeding up incident response times.”



Abhimanyu Das

Senior Cybersecurity Engineer at Kyndryl

- ✔ “Skyhawk Security has positively impacted my organization because we are a small security team, and Skyhawk Security allows us to prioritize our work.”



Amit Levran

Head of Security at SundaySky

- ✔ “Skyhawk Security has plenty of products and subscriptions available, and at this moment, Skyhawk Security appears to be the leading company in the cybersecurity area.”



Alexander Bershtansky

Cross Platform Development/Solutions Architect And Integrations at One1



“It helps us in reaching the ISO27001 certification.”



Christian Ferranti

Chief Technology Officer at Euclidea



“The initial setup process is easy and intuitive.”



John Jimenez

Cyber Security Analyst at a manufacturing company with 11-50 employees

What users had to say about valuable features:

“The solution offers quick notifications.

We get five-minute configuration and exportable reports. We have configured CNP in five minutes or less and after only 24 hours we were able to obtain the first insights useful to tune in our infrastructure.

After remediating a couple of problems, we started to configure Slack notifications, test the ISO27001 compliance, and starting to export a couple of reports. We use these reports in our periodic meetings with the steering committee to report the status of our infrastructure. .”

Christian Ferranti

Chief Technology Officer at Euclidea

[Read full review](#) 

“Regarding cyber attacks, I would be glad to recommend Skyhawk Security products. Skyhawk Security has plenty of products and subscriptions available. At this moment, Skyhawk Security appears to be the leading company in the cybersecurity area. There are different kinds of attacks, such as DDoS attacks and many other types. Many clients around the world are using this platform and it is proven and highly valued, which I totally agree with.

“I need to mention the outstanding service as well. The uniqueness and professional quality of the product are noteworthy. Skyhawk Security is a big company with many sites around the world that support the application and product itself. There is hardware and software, and everything works together. It is proven and solves the issues and does what it really needs to do.

“Skyhawk Security has artificial intelligence and AI capabilities. The real-time intelligence is connected to real-time detection. The machine learning and DevOps department are connected to this as well. Straightforward and effective, it is proven to work.

“Analytics capabilities allow me to analyze and check reports, check statuses, and review all issues in real time or historically. I count the issues, the percentage of solved issues, non-solved issues, how quickly I am catching vulnerabilities, and so on..”

Alexander Bershtansky

[Read full review](#) 

Cross Platform Development/Solutions Architect And Integrations at One1

“The best features Skyhawk Security offers are the ability to prioritize your work, especially when you have limited staff, and ensure that you address the most important issues first and with urgency. A security team is usually very thin-spread and doesn't have a lot of resources to solve issues. Skyhawk allows me to prioritize those based on the actual probability of a vulnerability being exploited.

“Skyhawk Security helps me prioritize through the dashboards. They have a dashboard that shows me the amount of vulnerabilities that I have. From those vulnerabilities, it lists out the ones that are exploitable. From the ones that are exploitable, it shows me the ones that are weaponizable and how they are weaponizable. From there, it shows me the ones that are weaponizable and have the ability to impact my Crown Jewels.

“Skyhawk Security has positively impacted my organization because we are a small security team, and Skyhawk Security allows us to prioritize our work. We are better at what we do, and it doesn't take more people to do more important work. With the limited staff that we have, we are able to address the things that pose the highest risk to us first, rather than take all the critical vulnerabilities and address them one by one without any type of prioritization.

“Our outcomes since using Skyhawk Security changed because we went down from thousands of vulnerabilities that we needed to review and address to a prioritized list that includes a handful of vulnerabilities that we needed to fix because they were the most urgent. We then have a work plan to address all the others. From a focus perspective, it improved the focus of my team, and it improved the efficiency and effectiveness of my team because we are now addressing the most urgent issues first..”

Amit Levran

Head of Security at SundaySky

[Read full review](#) 

“Skyhawk Security helps me cut through false positives primarily through its machine learning based on behavior analysis that creates a personalized model for our specific cloud environment, applications, and users. Alerts only fire when something is actually abnormal and not just triggered on every minor abnormality. The key feature that makes this easier is how it aggregates multiple suspicious events into what they call malicious behavior indicators, then correlates those activities and attack sequences before raising an alert.

“What really stands out about Skyhawk Security compared to other solutions I have used is its focus on weaponized attacks and exploit verification rather than just finding vulnerabilities and misconfigurations. Most tools such as Wiz or other CSPM platforms will tell you about thousands of CVSS security issues, but Skyhawk validates which vulnerabilities are actually weaponized and which real attacks can be explained in the specific environment context. Another unique aspect is how it integrates with AI to fight AI-driven attacks, which is becoming increasingly important as attackers now use AI to automate their attacks. The explainability built into every alert means I not only know what happened, but why it is a threat and how the attack unfolded, making my investigation work much faster compared to other solutions where I had to manually piece together attack timelines. This allows me to focus on genuine critical threats by filtering out noise and gives me the confidence that I am prioritizing based on actual exploits rather than just theoretical vulnerability vectors.

“The best features in Skyhawk Security that I find most valuable include the AI-powered automation of purple team simulations that create a digital twin of our cloud environment. I use the automation of the purple team the most because it continuously runs attack simulations against our actual cloud setup without impacting production, validating whether vulnerabilities are truly exploited or weaponized before attackers exploit them. In my daily activities, the real observability in real-time provides evidence in one place for many unfolding threats. Additionally, the risk scoring system alerts me based on exploitability and is superb since it completes in minutes without requiring additional agents across our cloud workloads. It saves time and reduces complexity. Overall, the combination of continuous proactive protection through attack simulation and real-time threat detection with full context is what makes Skyhawk Security stand

out compared to other tools I have used.

“The digital twin makes my day-to-day tasks significantly easier and helps me spot vulnerabilities faster by giving me a completely virtual replica of our cloud environment where I can test attack scenarios safely without touching production. What makes it so valuable is that it continuously simulates how an attacker would move through our actual cloud infrastructure, allowing me to instantly tell the difference between critical vulnerabilities and low-risk issues in production versus development. This allows me to prioritize remediation based on actual business impacts rather than just CVSS scores..”

Abhimanyu Das

Senior Cybersecurity Engineer at Kyndryl

[Read full review](#) 

Other Solutions Considered

I have used multiple tools, including various EDR and EPP tools, as I have worked on implementation projects for those solutions. I mainly have experience with multiple tools, and one of the customer requirements was to work with Skyhawk Security.

Abhimanyu Das

Senior Cybersecurity Engineer at Kyndryl

[Read full review](#) 

“I previously used a different solution, but I prefer not to mention the name of the previous solution. We switched because that solution wasn't giving us a breakdown of which vulnerabilities are actually weaponizable. They were looking at toxic combinations, and a toxic combination is not necessarily exploitable and not necessarily weaponizable. We switched to Skyhawk Security because it gives us better visibility and better understanding of the vulnerabilities..”

Amit Levran

Head of Security at SundaySky

[Read full review](#) 

ROI

Real user quotes about their ROI:

I have already mentioned that it reduces alerts by 90%, which saves us time and provides cost-cutting benefits. So from that perspective, you can say it is a good return on investment.

Abhimanyu Das

Senior Cybersecurity Engineer at Kyndryl

[Read full review](#) 

“I have seen a return on investment; the metrics are less about fewer employees needed because my team is two employees. The return on investment is not a matter of fewer employees needed. There is ongoing work in the security field, and we are doing better work. We are more effective and more efficient in how we do things. The amount of time it takes us to get to critical issues that are dangerous to our environment is a lot shorter now than what it used to be..”

Amit Levran

Head of Security at SundaySky

[Read full review](#) 

Use Case

“I have moved to another niche and switched to work with the Oracle Cloud platform. I need clarification on the scenario and case regarding Oracle Cloud and Oracle Fusion, specifically what the request or issue is..”

Alexander Bershtansky

Cross Platform Development/Solutions Architect And Integrations at One1

[Read full review](#) 

“We use it to check compliance with iso27001. We have a full AWS environment and we need to stay updated with the derive of our infrastructure from ISO best practices.

Through CNP we are able, even if we are a small team, to be notified if something change and to remediate it in a short time.

We also use exportable reporting for our periodic meeting with the steering committee to update it about the status of our infrastructure. We use notifications through Slack and for use is very convenient to be notified in this way.”

Christian Ferranti


Chief Technology Officer at Euclidea

[Read full review](#) 

“My main use case of Skyhawk Security is cutting through the massive volume of alerts I deal with daily in my SOC operation. I primarily use it to validate which cloud vulnerabilities are actually exploited and weaponized before attackers can exploit them, so I can focus on real threats instead of chasing thousands of false positives from our Microsoft Sentinel and Defender alerts. The automation of purple team features lets me simulate real attacks against our cloud environment without touching production, which helps me prioritize remediation based on actual business risk rather than just CVSS score. This especially helped me when I was handling 10 to 15 tickets daily and I needed to quickly identify which ones were genuinely weaponized and which threats could impact our critical cloud assets. Basically, I use it to trust but verify our security alerts, making sure I'm spending my time on incidents that actually matter instead of chasing noise..”

Abhimanyu Das

Senior Cybersecurity Engineer at Kyndryl


[Read full review](#) 

“Skyhawk Security helps me identify threats in the cloud and misconfigurations in my environment and prioritize vulnerabilities based on their severity, but also based on the probability of a vulnerability being weaponized against my system.

“Skyhawk Security processes all the vulnerabilities that are identified by my CSPM, which is Wiz. They take tens, sometimes hundreds of thousands of vulnerabilities, and they help me identify the ones that are exploitable. From those, they identify the ones that are weaponizable against my system. They also let me know which of the weaponizable vulnerabilities can affect some of our most important assets, which they call Crown Jewels..”

Amit Levran

Head of Security at SundaySky

[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 integration with Skyhawk Security has been pretty smooth overall. It was relatively easy to connect with the other tools we already use because it is designed to work with existing security platforms without requiring agents and major infrastructure changes. What made it smoother is that it is a software-as-a-service based platform where we just confirm the API connection.

Abhimanyu Das

Senior Cybersecurity Engineer at Kyndryl

[Read full review](#) 

Customer Service and Support

“The customer support for Skyhawk Security is great. There is a dedicated team that works with you. We have weekly calls. They are very responsive. In some cases, they released features within a few days, sometimes weeks, when we needed them. They are very attentive to customers, they listen to the market, and they listen to their customers. They are very market-oriented and their goal is to build a product that creates value for their customers..”

Amit Levran

Head of Security at SundaySky

[Read full review](#) 

Other Advice

“It is a matter of competitors and what the product gives to me. The value is worth it when I am getting the value from the price. Regarding the price, every customer can say that the price should be lower, but indeed the product is working very well. I think the value is worth it. I prefer working less with competitors and talking less about competitors. I rate this review a ten out of ten..”

Alexander Bershtansky

Cross Platform Development/Solutions Architect And Integrations at One1

[Read full review](#) 

“I can view the alarms within the platform and subsequently implement various security measures in response. It assists with incident response by providing alerts and visual representations of different security events. However, the effectiveness can vary, and sometimes more effort is required for resolution.

DDoS attacks, including detection of DTO POS and identification of malicious IPs, are critical aspects of security to ensure the availability and performance of your systems.

The real-time monitoring feature provides enough services to meet the requirements of our security infrastructure.

I rate Redware Cloud Native Protector a ten out of ten..”

John Jimenez

Cyber Security Analyst at a manufacturing company with 11-50 employees

[Read full review](#) 

“The advice I would give to others looking into using Skyhawk Security is to always understand what the impact of your tool is on your organization and not just what the tool shows you. There are a lot of tools in the market that are looking to increase the number of vulnerabilities and the number of findings to prove that they are doing something and identifying risks or vulnerabilities. When those vulnerabilities are identified, ensure that you are able to address them in some type of order, and that order is based on your needs and not on the need to show a large number of vulnerabilities.

“Skyhawk Security also has a CDR, a Cloud Detection and Response feature, that allows identification of abnormal activity in the cloud environment.

“I purchased Skyhawk Security through the [AWS Marketplace](#).

“I would rate this product a 9 overall..”

Amit Levran

Head of Security at SundaySky

[Read full review](#) 

“Skyhawk Security has had a really positive impact on our organization, especially in reducing false positives and speeding up incident response times. We have seen a dramatic reduction in alert volume, with customers using Skyhawk Security reporting around a 99% reduction in [CNAPP](#) alert noise. This means instead of drowning in thousands of daily alerts, our SOC team is now focusing on just 1% of alerts that actually matter. This has saved us weeks to months in remediation time because we are not wasting resources chasing false positives or addressing vulnerabilities that pose no real threat.

“While we have not tracked the exact numbers yet, we have seen our incident response time drop from around four to five hours to under 30 minutes for most alerts, which is a huge improvement. The biggest win is the reduction in false positives; instead of investigating 10 to 15 alerts per ticket, I am now looking at maybe one to two validation threats. I estimate we have saved about 60 to 70%

time on alert triage, translating to probably 8 to 10 hours saved per week for me personally, which adds up to weeks of saved time across the whole team over a year. The ability to validate responses on the digital twin before deploying them also cuts our testing time from days to hours when creating new playbooks, allowing us to chase exploits much faster instead of waiting for attackers to find them first.

“A small detail I really appreciate about Skyhawk Security that I have not mentioned yet is how the platform explains every alert with clear actionable context, detailing exactly why something is a threat and what an attacker could do next. As someone who has been in SOC operations for about 8 to 10 years, dealing with [Microsoft Sentinel](#) and Defender, I am used to alerts that just notify me of something suspicious without much detail. Skyhawk Security walks me through the whole attack story with built-in evidence, so I do not have to waste time digging through logs and piecing things together myself. I also appreciate how it integrates with the tools I already use without requiring major changes to our workflow, which makes adoption smoother for our team. The platform updates continuously as our cloud environment changes, so I never have to worry about testing outdated configurations or missing newly added assets. The fact that it is agentless and can be up and running in our environment in minutes instead of weeks was a huge plus since we did not have to deal with deploying and managing agents across our setup. These smaller details might seem minor, but they add up, saving me real time and reducing mental load while juggling multiple security tickets throughout the day.

“My advice for others looking into using Skyhawk Security is that it will reduce your time and minimize your alerts for false positives, helping you a lot in the future. I rate this solution an 8 out of 10..”

Abhimanyu Das

Senior Cybersecurity Engineer at Kyndryl

[Read full review](#) 

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